

# THESE

présentée à

L'UNIVERSITE PIERRE ET MARIE CURIE (PARIS VI)

pour l'obtention du

DOCTORAT D'ETAT ES SCIENCES

Spécialité: MATHEMATIQUES

Mention: INFORMATIQUE

par M. Christophe REUTENAUER

Sujet de la thèse: séries rationnelles et algèbres syntactiques

Soutenue le 16 avril 1980 devant la Commission

composée de: Président M. M.-P. SCHUTZENBERGER

Examineurs: MM. J. BERSTEL  
A. ERUNEL  
M. FLIESS

Invites: P.M. COHN



# THESE

présentée à

L' UNIVERSITE PIERRE ET MARIE CURIE (PARIS VI)

pour l'obtention du

DOCTORAT D'ETAT ES SCIENCES

Spécialité: MATHEMATIQUES

Mention: INFORMATIQUE

par M. Christophe REUTENAUER

Sujet de la thèse: séries rationnelles et algèbres syntactiques

Soutenue le 16 avril 1980 devant la Commission

composée de: Président M. M.-P. SCHUTZENBERGER

Examineurs: MM. J. BERSTEL  
A. BRUNEL  
M. FLIESS

Invites: P.M. COHN



## Geneviève



*L'auteur remercie*

*Monsieur le Professeur Schützenberger, précurseur dans ce domaine,  
qui a accepté de présider ce jury*

*Monsieur le Professeur Cohn qui, par sa présence, manifeste l'intérêt  
qu'il porte au présent sujet de recherche*

*Monsieur le Professeur Brunel, qui m'a proposé cet intéressant sujet  
de deuxième thèse (le théorème d'isomorphisme entre schémas de Bernoulli,  
de Keane et Smorodinsky)*

*Michel Fliess, dont d'anciens travaux ont jeté les bases de la  
présente thèse, et qui s'est toujours intéressé à ce travail*

*Monsieur le professeur Jean Berstel enfin, dont la direction libérale,  
amicale et encourageante a créé d'excellentes conditions de travail.*

*La frappe de cette thèse a été effectuée par Mmes Beaujean  
et Chaumard, de l'Institut de Programmation, et Mme Beaumer, de  
Montgeron; l'impression et l'édition ont été réalisées à l'imprimerie  
de l'Institut de Programmation par Mmes Le Floch, Angot et Marguillard  
et Mrs Couvreur et Couvigny.*

*Et mon ami Etienne Sag a dessiné les illustrations.*



séries rationnelles et  
algèbres syntactiques

christophe reutenauer



## INTRODUCTION

Les séries formelles furent employées d'abord par Monsieur Schützenberger (1961) pour l'étude fine des langages formels. A sa suite cet emploi des séries formelles en théorie des langages a connu un vaste développement et a donné naissance à une théorie des séries rationnelles et algébriques en variables non commutatives. Le présent travail constitue une contribution à cette théorie.

Les applications des séries formelles sont multiples : il y a par exemple, la théorie énumérative des graphes, initiée par Cori et Richard (1972) ; il y a aussi l'automatique non linéaire, où Fliess (1976) a introduit l'emploi des séries formelles pour la réalisation des asservissements ; et encore l'étude itérative des endomorphismes du monoïde libre où les séries formelles jouent un rôle important pour l'examen des DTOL-systèmes (cf. Salomaa-Soittola 1977).

Les interactions entre séries rationnelles et langages rationnels sont plus que fréquentes. Notamment, les séries rationnelles constituent le cadre adéquat pour les problèmes de multiplicité et d'ambiguïté (voir l'ouvrage de Monsieur Eilenberg 1974 pour un exposé systématique de ce point de vue). Sans aller jusqu'à prétendre que les séries formelles occupent dès maintenant vis-à-vis des langages la place que prend la théorie des nombres par rapport à l'arithmétique élémentaire ("arithmetization of automata and language theory" A. Salomaa op. cit.), nous pensons qu'une étude attentive des conséquences sur les langages des propriétés des séries rationnelles apporte des résultats neufs et un éclairage fécond ; un exemple frappant de ce fait nous est fourni par les travaux de Fliess (1974b) sur les langages stochastiques : il y utilise des résultats de théorie des nombres (approximation diophantienne) pour répondre par la négative à des questions de fermeture de ces langages.

J'espère avoir contribué à illustrer ce point de vue dans le présent travail.

Depuis son apparition en informatique théorique, la théorie des séries rationnelles a puisé son inspiration à deux sources : d'une part, comme déjà dit, à la théorie des langages, et d'autre part à celle des fonctions rationnelles d'une variable complexe ; ce dernier point de vue a conduit à examiner des propriétés arithmétiques de leurs coefficients (voir Pólya

et Szegő 1964). Ainsi toute une problématique issue de l'étude arithmétique des suites définies par une relation de récurrence linéaire (étude qui a intéressé de nombreux chercheurs) se retrouve dans l'étude des séries rationnelles en variables non commutatives. Et la théorie des langages y trouve son compte, puisque (par exemple) une notion purement arithmétique comme, pour un ensemble d'entiers, de n'avoir qu'un nombre fini de diviseurs premiers se révèle être équivalente à celle de non-ambiguïté (et se révélerait encore plus si j'avais pu résoudre ma conjecture dans tous les cas, chapitre VI). Par ailleurs, le point de vue adopté dans l'étude des séries rationnelles a conduit à l'étude spécifique des séries  $\mathbb{N}$ -rationnelles ; et les séries  $\mathbb{N}$ -rationnelles d'une variable se sont avérées n'être pas autre chose (essentiellement) que les suites de Pisot, les suites définies par une relation de récurrence linéaire ayant une racine dominante (théorème de Berstel, voir Eilenberg 1974, et sa réciproque, de Soittola).

Jusqu'alors les outils employés dans l'étude des séries formelles s'inspiraient des deux sources : techniques combinatoires d'une part, techniques linéaires, arithmétiques et analytiques d'autre part. Notre contribution s'en différencie essentiellement par l'utilisation systématique d'outils algébriques. Cette méthodologie, outre le fait qu'elle apporte une meilleure compréhension de la nature des objets, permet d'apporter des réponses nouvelles à des questions qui ne semblaient pas être accessibles par les moyens précédemment employés.

Ce travail est divisé en huit chapitres. Le premier commence par introduire certaines notions de base : demi anneaux, séries formelles etc...

Au passage, nous relevons une propriété amusante de l'étoile d'une série, qui permet une définition plus générale de cette opération ; nous montrons aussi que la continuité des morphismes de séries formelles est liée à des questions de nilpotence. Mais le point le plus important de ce chapitre est une étude originale de l'algèbre des séries rationnelles en une variable ; elle est très technique, mais permettra des raisonnements rapides dans la suite, et d'obtenir des résultats nouveaux.

Au chapitre deux nous introduisons notre outil principal : l'algèbre syntactique. Cette notion est l'analogue, pour les séries formelles, de la notion de monoïde syntactique pour les langages. Elle permet notamment une jolie formulation du théorème de Kleene-Schützenberger : Une série est rationnelle si et seulement si son algèbre syntactique est de dimension finie.

Ainsi commence le chapitre trois, qui continue en présentant un critère de rationalité des séries formelles et un autre pour les langages : ils s'appuient tous deux sur un théorème de Chirchov dans les algèbres à identité polynômiale et ainsi, les problèmes de rationalité s'inscrivent naturellement dans le cadre (ou juste à côté) des problèmes classiques de Burnside et de Kurosch. Un corollaire curieux de celà est une propriété des langages rationnels liée aux identités polynômiales standards d'Amitsur-Levitzki : un langage rationnel est, en un sens, faiblement commutatif. Dans ce même chapitre, nous construisons pour les idéaux bilatères de l'algèbre associative libre des systèmes de générateurs particuliers, liés à certains codes bipréfixes et obtenons ainsi des relations de récurrence linéaires bilatères pour les séries rationnelles. Ensuite nous caractérisons les séries rationnelles centrales (i.e. celles dont le coefficient d'un mot ne dépend que de sa classe de conjugaison) et puis les algèbres syntactiques de celles d'entr'elles qui sont des caractères.

Au chapitre quatre, nous utilisons le critère de rationalité précédemment établi pour l'étude approfondie de deux problèmes : celui des extensions de Fatou et celui du quotient de Hadamard. Pour le premier, nous caractérisons les extensions de Fatou des anneaux commutatifs intègres, et les anneaux de Fatou faibles, étendant ainsi au cas non commutatif un théorème de Cahen et Chabert. Quant au second, nous étendons un résultat de Lamèche et Jacob à un grand nombre de cas nouveaux.

Le chapitre suivant (numéro cinq) est consacré par l'étude des pseudovariétés d'algèbres de dimension finie en relation avec les variétés de séries rationnelles. Il s'y établit tout d'abord un théorème de correspondance entre ces deux types de variétés, analogue à celui d'Eilenberg sur les pseudovariétés de monoïde finis. La suite du chapitre consiste à amorcer une étude de certaines variétés : variétés littérales, fermées par produit, par produit de Hadamard, équationnelles. Le résultat principal est l'analogue

pour les séries formelles du théorème de Schützenberger sur les monoïdes sans périodes, et dit à peu près ceci : une série rationnelle appartient à l'algèbre engendrée par les lettres et les séries (dites) géométriques si et seulement si tous les quotients simples de son algèbre syntactique sont isomorphes au corps de base.

Le chapitre six est dominé par des conjectures concernant les propriétés arithmétiques des coefficients d'une série rationnelle. Ainsi il y aurait équivalence, pour une série rationnelle, entre :

- (i) n'avoir dans ses coefficients qu'un nombre fini de diviseurs premiers
- (ii) être inversible dans l'algèbre de Hadamard, et
- (iii) être rationnelle non ambiguë.

Nous résolvons ces conjectures dans des cas particuliers. Cependant, nous étendons au cas de la caractéristique quelconque un théorème de Benzaght sur les séries rationnelles d'une variable qui sont Hadamard inversibles et celà, par une démonstration entièrement algébrique (celle de Benzaght utilisait l'analyse, ce qui rendait inaccessible l'étude de la caractérisation  $p$ ).

Le chapitre sept concerne les langages qui sont supports de séries rationnelles. Nous établissons un lemme d'itération pour ces langages, semblable, dans sa formulation, à un lemme d'Ogden. Un lemme analogue existe pour les langages rationnels mais sa preuve est évidente : il suffit de remarquer que, dans un graphe fini, tout chemin assez long contient une boucle. Pour les demi-groupes de matrices, la notion de boucle est remplacée par celle de matrice pseudo-régulière, comme l'avait remarqué Jacobson et ici, la finitude du graphe est remplacée par la finitude de la dimension de l'algèbre extérieure d'un espace vectoriel de dimension finie. Une application est que la famille des supports des séries  $K$ -rationnelles ( $K$  un sous-demi-anneau de  $\mathbb{R}$ ) est un cône rationnel fermé pour les opérations rationnelles (full AFL) ; la seule difficulté est en fait de montrer que cette famille est fermée par morphisme direct, ce que nous faisons ici. Enfin, nous soulevons la question suivante : Que peut-on dire de deux langages complémentaires qui sont tous deux supports de séries rationnelles ? Les seuls exemples connus sont les langages rationnels, je conjecture qu'ils le sont toujours. Nous montrons qu'il en est ainsi pour une variable (ce qui n'est nouveau qu'en caractéristique  $p$ ). Par ailleurs, dans le cas général, nous montrons que le monoïde syntactique de tels langages est de torsion.

Le chapitre huit est à part des précédents (en ce sens que le mot syntactique ne s'y trouve pas écrit). Il traite de séries associées aux DTOL-systèmes, qui sont considérés ici comme des homomorphismes d'un monoïde libre dans le monoïde des endomorphismes d'un autre monoïde libre. De cette manière, on peut associer à toute série sur le second une série sur le premier. Nous montrons que l'image par cette application d'une série rationnelle à croissance polynômiale est une série rationnelle.

Une partie des chapitres II, III, IV, et V est à paraître dans Journal of Algebra.

Une partie du chapitre VI a fait l'objet d'une communication (1979 a) au Congrès FCT'79 à Berlin (Hauptstadt der DDR). Une partie du chapitre VII (§ 1 et 2) est à paraître dans Acta Informatica et le chapitre VIII est paru intégralement dans Theoretical Computer Science (1979).



7

PLAN

|                     |                                                       |    |    |
|---------------------|-------------------------------------------------------|----|----|
| <u>Chapitre I</u>   | <u>Préliminaires.</u>                                 | 9  |    |
| 1.                  | Demianneaux                                           | 10 |    |
| 2.                  | Séries formelles                                      | 12 |    |
| 3.                  | Séries reconnaissables                                | 14 |    |
| 4.                  | Séries rationnelles                                   | 21 |    |
| 5.                  | La guerre des étoiles                                 | 21 |    |
| 6.                  | Morphisme de séries formelles                         | 24 |    |
| 7.                  | Relations de récurrence linéaires à droite            | 29 |    |
| 8.                  | Séries rationnelles régulières                        | 31 |    |
| 9.                  | Séries rationnelles d'une variable                    | 32 |    |
| <br>                |                                                       |    |    |
| <u>Chapitre II</u>  | <u>Algèbres syntactiques.</u>                         | 41 |    |
| 1.                  | Représentation d'une série formelle                   | 43 |    |
| 2.                  | Liens avec le module sériel                           | 50 |    |
| 3.                  | Liens avec les langages                               | 54 |    |
| 4.                  | Changement d'anneau                                   | 57 |    |
| <br>                |                                                       |    |    |
| <u>Chapitre III</u> | <u>Algèbres syntactiques des séries rationnelles.</u> |    | 61 |
| 1.                  | Le théorème fondamental                               | 64 |    |
| 2.                  | Un théorème de Chirchov                               | 70 |    |
| 3.                  | Un critère de rationalité                             | 72 |    |
| 4.                  | Relations de récurrence linéaires bilatères           | 77 |    |
| 5.                  | Séries rationnelles centrales                         | 86 |    |
| <br>                |                                                       |    |    |
| <u>Chapitre IV</u>  | <u>Applications.</u>                                  | 93 |    |
| 1.                  | Extensions de Fatou                                   | 94 |    |
| 2.                  | Un quotient de Hadamard                               | 98 |    |

Chapitre V Variétés.

109

- |                                                         |     |     |
|---------------------------------------------------------|-----|-----|
| 1. Le théorème des variétés                             | 111 |     |
| 2. Quelques variétés particulières                      | 117 |     |
| 3. Variétés littérales                                  | 120 |     |
| 4. Variétés fermées par produit                         | 122 |     |
| 5. Variétés fermées par produit de Hadamard, de Hurwitz |     | 133 |
| 6. Variétés équationnelles                              | 138 |     |

Chapitre VI Séries de Pólya.

143

- |                                     |     |
|-------------------------------------|-----|
| 1. Séries rationnelles non ambiguës | 145 |
| 2. Séries de Pólya                  | 150 |
| 3. Sur l'inverse de Hadamard        | 161 |

Chapitre VII Supports.

167

- |                                      |     |
|--------------------------------------|-----|
| 1. Le théorème d'itération de Jacob  | 169 |
| 2. Un lemme d'itération "à la Ogden" | 174 |
| 3. Applications                      | 180 |
| 4. Complémentation                   | 184 |
| 5. Extension                         | 189 |

Chapitre VIII Sur les séries associées à certains systèmes de Lindenmayer

- |                                                   |     |
|---------------------------------------------------|-----|
| 1. Séries N-rationnelles à croissance polynômiale | 192 |
| 2. DTOL-séries                                    | 197 |
| 3. Exemple                                        | 201 |

## CHAPITRE I - PRELIMINAIRES

Nous commençons par présenter certaines notions de bases : demi-anneaux, séries formelles, reconnaissables et rationnelles et énonçons sans preuve quelques unes de leurs propriétés fondamentales (paragraphe 1, 2, 3, 4). Les paragraphes 5 et 6 sont consacrés à l'étude de transformations particulières des séries, à savoir l'étoile et les morphismes. Notre définition de l'étoile d'une série, qui semble être la plus naturelle, étend les définitions habituelles et conserve cependant la rationalité. Nous caractérisons les morphismes de séries et montrons qu'ils conservent la rationalité, ce qui nous permet en particulier de prouver simplement un résultat de Jacob sur les transductions régulières. Au paragraphe 7 nous étendons au cas des anneaux les relations de récurrence linéaires des séries rationnelles, comme les a établies Schützenberger dans le cas des corps. Enfin, au paragraphe 9, nous rappelons un certain nombre de propriétés classiques des suites qui vérifient une relation de récurrence linéaire (i.e. les séries rationnelles d'une variable) ; ensuite, nous établissons une propriété remarquable de ces suites : il s'agit essentiellement de ramener l'étude de l'algèbre de Hadamard de ces suites à celle de l'algèbre d'un groupe abélien libre.

## 1. DEMIANNEAUX

Un *demianneau*  $K$  est un ensemble muni de deux lois  $+$  et  $\cdot$  vérifiant :

- \*  $(K, +)$  est un monoïde commutatif dont l'élément neutre est noté 0.
- \*  $(K, \cdot)$  est un monoïde dont l'élément neutre est noté 1.
- \* La multiplication est distributive par rapport à l'addition.
- \* On a  $0 \cdot k = k \cdot 0 = 0$  pour tout  $k \in K$ .

Le demianneau  $K$  est dit *commutatif* si la multiplication  $\cdot$  est commutative. On définit les *morphismes de demianneaux* de manière évidente : le point important est qu'ils conservent 0 et 1. Un *sous-demianneau* de  $K$  est un demianneau  $K'$  contenu dans  $K$  et tel que l'injection  $K' \rightarrow K$  soit un morphisme de demianneaux.

Un  $K$ -module à droite  $M$  est un ensemble muni d'une loi interne et d'une loi externe  $M \times K \rightarrow M$ , notée  $(m, k) \mapsto mk$ , telles que

‡  $(M, +)$  est un monoïde commutatif dont l'élément neutre est noté 0

‡ On a, pour  $k, l \in K$ ,  $m, n \in M$ , les relations :

$$(m + n)k = mk + nk \qquad (m \cdot k)l = m(kl)$$

$$m(k + l) = mk + ml \qquad m \cdot 1 = m$$

$$m \cdot 0 = 0 \qquad 0 \cdot k = 0.$$

Un  $K$ -module est dit de *type fini* s'il admet un système générateur fini. On définit les *formes linéaires*  $M \rightarrow K$  de manière usuelle ; de même les homomorphismes et les endomorphismes de  $K$ -modules.

Exemple 1 (i) Le *demianneau de Boole*, noté  $\mathcal{B}$ , est réduit aux deux éléments 0 et 1, avec la relation  $1 + 1 = 1$ .

(ii)  $\mathbb{N}$ ,  $\mathbb{Q}_+$ ,  $\mathbb{R}_+$ ,  $\mathcal{N}^0$  (obtenu à partir de  $\mathbb{N}$  par l'adjonction de  $\infty$ , avec :  $\forall a \in \mathcal{N}^0$ ,  $a + \infty = \infty$  et si  $a \neq 0$ ,  $a \infty = \infty$ ) sont des demi-anneaux qui ne sont pas des anneaux.

(iii) Un demianneau  $K$  est dit *positif* si d'une part  $a + b = 0$  implique  $a = b = 0$  et d'autre part  $ab = 0$  implique  $a$  ou  $b = 0$ . Autrement dit l'application  $K \rightarrow \mathcal{B}$  définie par  $0 \mapsto 0$ ,  $K \setminus 0 \mapsto 1$  est un morphisme de demianneaux.

Un demianneau est dit *régulier* si  $a + b = a + c$  implique  $b = c$  (autrement dit, il est plongeable dans un anneau). Il est dit *intègre* si  $ab = 0$  implique  $a$  ou  $b = 0$  et *simplifiable* si  $ab = ac$  implique  $a = 0$  ou  $b = c$  (Le lecteur curieux pourra vérifier qu'il ne suffit pour un demianneau commutatif d'être régulier et simplifiable pour qu'on puisse le plonger dans un corps ; mais que la condition nécessaire et suffisante pour qu'il en soit ainsi est qu'il soit régulier et que

$$ac + bd = ad + bc \text{ implique } a = b \text{ ou } c = d).$$

Si  $P$  et  $Q$  sont deux ensembles on note  $K^{P \times Q}$  l'ensemble des matrices de dimension  $P \times Q$  à coefficients dans  $K$  ;  $K^{P \times Q}$  est naturellement muni d'une structure de  $K$ -module à gauche et à droite. Si  $R$  est un autre ensemble et  $Q$  est fini, on peut définir le produit d'un élément de  $K^{P \times Q}$  par un élément de  $K^{Q \times R}$ , de manière usuelle : c'est un élément de  $K^{P \times R}$ . Si  $Q$  est fini,  $K^{Q \times Q}$  devient ainsi un demianneau contenant  $K$  (si  $K$  est commutatif, on peut parler de  $K$ -algèbre ...). Si  $P = \{1, \dots, r\}$  et  $Q = \{1, \dots, s\}$  on note  $K^{P \times Q}$  aussi par  $K^{r \times s}$ .

## 2. SERIES FORMELLES

Soit  $K$  un demi-anneau et  $X$  un alphabet (non nécessairement fini). Une *série formelle* sur  $X$  à coefficients dans  $K$  est une application  $X^* \rightarrow K$ , c'est-à-dire un élément de  $K^{X^*}$  que nous notons aussi  $K \langle\langle X \rangle\rangle$ . Si  $S \in K \langle\langle X \rangle\rangle$  et  $w \in X^*$ , on note  $(S, w)$  l'image du mot  $w$  par la série formelle  $S$ , et on l'appelle aussi *coefficient de  $w$  dans  $S$* . On écrit alors

$$S = \sum_{w \in X^*} (S, w) w$$

ce qui se justifie de la manière suivante :

tout d'abord, il existe une injection canonique  $X^* \rightarrow K \langle\langle X \rangle\rangle$  et  $K \langle\langle X \rangle\rangle$  est muni naturellement d'une structure de  $K$ -module à droite et à gauche (de bimodule en fait...) et les mots commutent aux scalaires, i.e.  $kw = wk$  si  $k \in K$  et  $w \in X^*$  : le terme  $(S, w)w$  désigne le produit à gauche du scalaire  $(S, w)$  par la série formelle  $w$  (ce terme est égal d'ailleurs à  $w(S, w) \dots$ ). En outre, on munit  $K$  de la topologie discrète et  $K \langle\langle X \rangle\rangle = K^{X^*}$  de la topologie produit ; dans  $K \langle\langle X \rangle\rangle$ , une famille  $(S_i)_{i \in I}$  est sommable dès qu'elle est *localement finie*, i.e. pour tout mot  $w$  l'ensemble des  $i$  tels que  $(S_i, w) \neq 0$  est fini. De même, on munit  $K$  de la structure uniforme discrète et  $K \langle\langle X \rangle\rangle$  de la structure uniforme produit :  $K \langle\langle X \rangle\rangle$  devient ainsi un espace uniforme complet. La famille des séries  $((S, w)w)_{w \in X^*}$  est clairement localement finie, donc sommable, et sa somme est  $S$ . D'où la relation ci-dessus.

Le *support* d'une série  $S$  est le langage

$$\text{supp}(S) = \{ w \in X^* \mid (S, w) \neq 0 \}$$

Un *polynôme* est une série formelle de support fini, c'est-à-dire un élément de  $K^{(X^*)}$ , qu'on note aussi  $K \langle X \rangle$ .

Lorsque l'alphabet  $X$  est fini (hypothèse que nous ferons le plus souvent) la topologie et la structure uniforme définies ci-dessus sont métrisables, et même ultramétrisables : on définit l'ordre de deux séries  $S$  et  $T$  par

$$\omega(S, T) = \inf \{ n \in \mathbb{N} \cup \infty \mid \exists w \in X^*, (S, w) \neq (T, w), |w| = n \}$$

où  $|w|$  désigne la longueur du mot  $w$ . Cet ordre définit une distance, de la manière suivante ( $\alpha$  désigne un nombre réel,  $0 < \alpha < 1$ ) :

$$d(S, T) = \alpha^{\omega(S, T)}$$

Dans le cas où  $X$  est fini<sup>†</sup>,  $K \langle X \rangle$  est dense dans  $K \ll X \gg$ .

Nous notons  $\omega(S) = \omega(S, 0)$ .

On a  $\lim S_n = 0$  si et seulement si  $\lim \omega(S_n) = \infty$ .

Revenons à l'algèbre : on définit sur  $K \ll X \gg$  le produit de Cauchy défini par

$$(ST, w) = \sum_{uv=w} (S, u) (T, v)$$

$K \ll X \gg$  devient ainsi un demi-anneau topologique qui contient  $K$  et  $K \langle X \rangle$  comme sous-demi-anneaux : l'élément neutre est la série formelle 1, réduite au seul mot vide.

On définit aussi le produit de Hadamard par

$$(S \otimes T, w) = (S, w) (T, w)$$

C'est une autre manière de munir  $K \ll X \gg$  d'une structure de demi-anneau, qui contient aussi  $K$  et  $K \langle X \rangle$  comme sous-demi-anneaux : l'élément neutre est la série formelle  $\sum_{w \in X^*} w$ . Si  $K$  est commutatif, le produit de Hadamard est commutatif.

<sup>†</sup> et même si  $X$  est infini

Si la série  $S$  vérifie  $(S, 1) = 0$ , nous dirons qu'elle est *propre* : dans ce cas nous définissons l'*étoile* de  $S$  par la somme de la famille localement finie  $(S^n)_{n \geq 0}$  :

$$S^* = \sum_{n \geq 0} S^n$$

On note  $S^+ = SS^* = S^*S$

Si  $K$  est un anneau  $S^* = (1 - S)^{-1}$ .

Soit  $L$  un langage : nous appelons *série caractéristique* de  $L$ , notée  $\underline{L}$ , la série  $\sum_{w \in L} w$ . Comme le lecteur l'aura déjà noté, nous notons  $w$  au lieu de  $\underline{w}$  si  $w$  est un mot.

L'image d'une série formelle  $S$  est l'ensemble

$$\text{Im}(S) = \{(S, w) \mid w \in X^*\}$$

Si  $K$  est commutatif, toute série formelle  $S$  définit sur  $K \langle\langle X \rangle\rangle$  une forme  $K$ -linéaire, notée  $P \mapsto (S, P)$  par

$$(S, P) = \sum_{w \in X^*} (S, w) (P, w)$$

Réciproquement, toute forme linéaire sur  $K \langle\langle X \rangle\rangle$  définit une série formelle : ainsi  $K \langle\langle X \rangle\rangle$  s'identifie au dual de  $K \langle X \rangle$ . Nous ferons souvent, dans ce travail, confusion entre une série formelle et la forme linéaire qu'elle définit sur  $K \langle X \rangle$ .

### 3. SERIES RECONNAISSABLES

Une série formelle  $S \in K \langle\langle X \rangle\rangle$  est dite *reconnaissable* s'il existe un entier  $n \geq 1$ , un morphisme de monoïdes  $\mu : X^* \rightarrow K^{n \times n}$  (multiplicatif) et des matrices  $\lambda \in K^{1 \times n}$ ,  $\gamma \in K^{n \times 1}$  tels que  $\forall w \in X^*$ ,  $(S, w) = \lambda \mu_w \gamma$ .  
(avec la convention  $K^{1 \times 1} = K$ ).

Dans ce cas, nous appelons le triplet  $(\lambda, \mu, \gamma)$  une *représentation linéaire* de  $S$ , de dimension  $n$ . Nous disons aussi que  $(\lambda, \mu, \gamma)$ , ou  $\mu$ , reconnaît  $S$ .

Si  $S$  est une série formelle et  $w$  un mot, nous définissons les séries formelles  $Sow$  et  $woS$  par

$$(Sow, u) = (S, wu), (woS, u) = (S, uw)$$

$$(\text{On note aussi } Sow = w^{-1} S, woS = Sw^{-1}).$$

On a les relations :

$$S o (w w') = (S o w) o w'$$

$$(w w') o S = w o (w' o S)$$

$$1 o S = S o 1 = S$$

$$w o (S o w') = (w o S) o w'$$

La dernière relation permet de définir  $w o S o w' : K \langle\langle X \rangle\rangle$  devient ainsi un  $X^*$ -bimodule...

Si  $K$  est commutatif,  $K \langle\langle X \rangle\rangle$  devient ainsi un  $K \langle X \rangle$ -bimodule : il suffit de prolonger par linéarité l'opération ci-dessus ; si  $P$  est un polynôme

$$S o P = \sum_{w \in X^*} (P, w) S o w$$

Lorsque nous parlerons d'une structure de  $K \langle X \rangle$ -module à droite sur  $K \langle\langle X \rangle\rangle$ , ce sera toujours de celle-ci.

Nous énonçons maintenant (le plus souvent sans preuve), pour référence ultérieure un certain nombre de résultats (dont bon nombre sont bien connus) concernant les séries reconnaissables.

Nous avons la caractérisation suivante des séries reconnaissables, essentiellement due à Fliess.

Proposition 1 Soit  $S \in K \langle\langle X \rangle\rangle$ . Les conditions suivantes sont équivalentes :

- (i)  $S$  est reconnaissable
  - (ii) Il existe un  $K$ -module à droite de type fini  $M$ , un élément  $m_0 \in M$ , un homomorphisme  $\gamma: X^* \rightarrow \text{End}(M)$  et une forme linéaire  $\varphi: M \rightarrow K$  tels que  $\forall w \in X^*, (S, w) = \varphi \circ \gamma_w(m_0)$ .
  - (iii) ( $K$  commutatif) Il existe un sous- $K \langle X \rangle$ -module à droite de  $K \langle\langle X \rangle\rangle$ , qui est un  $K$ -module de type fini et qui contient  $S$ .
  - (iv) ( $K$  commutatif) Il existe un  $K \langle X \rangle$ -module à droite  $M$  qui est un  $K$ -module de type fini, une forme  $K$ -linéaire  $\varphi: M \rightarrow K$  et un élément  $m_0 \in M$  tels que  $\forall w \in X^* (S, w) = \varphi(m_0 w)$
- Dans ce cas, on peut supposer dans (ii) et (iv) que  $M$  est un  $K$ -module libre.

Pour une preuve, on pourra consulter Fliess (1974, th. 2.1.1.), Jacob (1975 chap. XIII b) ou Salomaa et Soittola (1977 th. 3.1. chap. II), ou encore Reutenauer (1979 prop. 1 § 2).

Corollaire 1 Soit  $L$  un sous-demi-anneau de  $K$  tel que  $K$  soit un  $L$ -module à droite de type fini : i.e. il existe  $a_1, \dots, a_r \in K$  tels que tout  $a \in K$  s'écrive  $\sum a_i b_i$  avec des  $b_i$  dans  $L$ . Alors toute série  $K$ -reconnaissable  $S$  s'écrit  $\sum a_i S_i$  où les  $S_i$  sont des séries  $L$ -reconnaissables.

Preuve D'après la proposition 1, il existe  $M, m_0, \nu, \varphi$  comme dans (ii). On peut supposer que  $M$  est libre : soit  $m_1, \dots, m_n$  une base du  $K$ -module  $M$ . Alors  $M$  est engendré, comme  $L$ -module par les éléments  $m_i a_j, 1 \leq i \leq n, 1 \leq j \leq r$ .

De plus  $\text{End}_K(M) \subset \text{End}_L(M)$ . Pour tout  $i, 1 \leq i \leq n$ , il existe des éléments  $b_{i,j}, 1 \leq j \leq r$ , de  $L$  tels que

$$\varphi(m_i) = \sum_j a_j b_{ij}$$

Soit, pour  $1 \leq j \leq r$ ,  $\varphi_j$  l'application  $K$ -linéaire  $M \rightarrow K$  définie par  $\varphi_j(m_i) = b_{ij}$  ; elle existe puisque  $(m_i)$  est une base de  $M$ . Alors

$$\sum_{1 \leq j \leq r} a_j \varphi_j(m_i) = \sum_j a_j b_{ij} = \varphi(m_i) \text{ donc } \varphi = \sum a_j \varphi_j.$$

Soit  $S_j$  la série définie par  $(S_j, w) = \varphi_j \circ \nu w(m_0)$ .  $S_j$  est  $L$ -reconnaissable et l'on a  $S = \sum S_j$ .  $\square$

Corollaire 2 Dans les hypothèses du corollaire soit  $\varphi : K \rightarrow L$  une application  $L$ -linéaire à droite. Si  $S$  est une série  $K$ -reconnaissable, la série  $\varphi(S) = \sum_{w \in X^*} \varphi((S, w))w$  est  $L$ -reconnaissable.

Preuve  $S = \sum a_i S_i$ , où les  $a_i$  sont dans  $K$  et les  $S_i$  sont des séries  $L$ -reconnaissables. Alors  $\varphi(S) = \sum \varphi(a_i) S_i$  puisque  $(\varphi(S), w) = \varphi((S, w)) = \varphi(\sum a_i (S_i, w)) = \sum \varphi(a_i) (S_i, w)$  ; par suite  $S$  est  $L$ -reconnaissable.  $\square$

On retrouve ainsi plusieurs résultats bien connus.

Corollaire 3 (Schützenberger 1961 IV.2) Toute série 2-reconnaissable est différence de deux séries  $N$ -reconnaissables.

Corollaire 4 (ibid. III.A.4) Soit  $n \geq 1$  et  $i, j \in \{1, \dots, n\}$ .

Si  $S$  est une série  $K^{n \times n}$  - reconnaissable,  $S_{i,j} = \sum (S, w)_{i,j} w$  est  $K$  - reconnaissable.

Preuve  $K^{n \times n}$  contient  $K$  et c'est un  $K$ -module à droite de type fini.

Soit  $\varphi: K^{n \times n} \rightarrow K$  qui à une matrice  $m$  associe  $m_{i,j}$ ;  $\varphi$  est clairement  $K$  - linéaire à droite. Il suffit donc d'appliquer le corollaire 2.

Proposition 2 (Schützenberger 1962) Si  $K$  est commutatif, le produit de Hadamard de deux séries reconnaissables est encore reconnaissable.

Théorème 1 (Schützenberger 1961 II.B.1) On suppose que  $K$  est un corps commutatif. Soit  $S$  une série  $K$  - reconnaissable et  $(\lambda, \mu, \gamma)$  une représentation linéaire de  $S$  de dimension minimum  $n$  parmi les représentations linéaires de  $S$ . Il existe alors des matrices  $m_{i,j}$  et des mots  $u_i, v_j, 1 \leq i \leq n, 1 \leq j \leq n$  tels que pour tout mot  $w$ :

$$\mu w = \sum_{i,j} m_{i,j} (S, u_i w v_j)$$

Une représentation linéaire de  $S$  de dimension minimum est appelée une représentation linéaire réduite de  $S$ . Sa dimension est le rang de  $S$  (qui est égal à  $\infty$ , par définition, si  $S$  n'est pas reconnaissable).

Proposition 3 (Fliess 1974 th. 2.1.1) On suppose que  $K$  est un corps commutatif. Le rang d'une série  $S$  est égal au rang de la matrice de Hankel de  $S$ , i.e. la matrice d'ordre  $X^* \times X^*$  dont l'entrée  $(u, v)$  est égale à  $(S, uv)$ .

Corollaire 1 On suppose que  $K$  est le corps des fractions de l'anneau  $A$ . Soit  $S$  une série  $K$ -reconnaissable dont les coefficients sont dans  $A$ . Si  $(\lambda, \mu, \gamma)$  est une représentation linéaire réduite de  $K$ , elle est à dénominateur bornée, i.e. il existe  $d \in A \setminus 0$  tel que  $\forall w \in X^*$ ,  $d \mu w \in A^{n \times n}$ .

Corollaire 2 Soit  $S \in \mathbb{R} \langle\langle X \rangle\rangle$  une série reconnaissable à croissance polynômiale, i.e. il existe  $C, n \in \mathbb{R}$  tel que  $\forall w \in X^*$ ,  $| (S, w) | \leq C |w|^n$ . Alors toute représentation linéaire réduite  $(\lambda, \mu, \gamma)$  de  $S$  est à croissance polynômiale, i.e. il existe  $C' \in \mathbb{R}$  tel que  $\forall w \in X^*$ ,  $| \mu w | \leq C' |w|^n$ .

Corollaire 3 (Fliess 1974 prop. 2.2.1) Si  $L \supset K$  sont deux corps commutatifs, toute série  $L$ -reconnaissable à coefficients dans  $K$  est  $K$ -reconnaissable.

Corollaire 4 (Schützenberger 1961 IV. 4)

Si  $K$  est un corps commutatif et  $S$  une série  $K$ -reconnaissable d'image finie, alors  $\text{supp}(S)$  est un langage reconnaissable.

Remarque 1 Sontag (1976) montre que ce résultat est encore vrai lorsque  $K$  est un anneau commutatif, mais faux en général lorsque  $K$  n'est pas commutatif. Un exemple de Choffrut (1978a, p.207) montre que c'est faux en général lorsque  $K$  est un demi-anneau commutatif ; il reste le problème suivant : si  $K$  est un demi-anneau commutatif et  $L$  un langage dont la série caractéristique est  $K$ -reconnaissable,  $L$  est-il reconnaissable ?

Proposition 4 (Schützenberger 1961 IV. 3) Si  $L$  est un langage reconnaissable, sa série caractéristique est reconnaissable (quel que soit  $K$ ).

Proposition 5 Soit  $K$  un corps commutatif muni d'une valeur absolue  $|\cdot|$ . Si  $S \in K \langle\langle X \rangle\rangle$  est reconnaissable, il existe  $C \in \mathbb{R}$  tel que

$$\forall w \in X^*, |S(w)| \leq C^{|w|}$$

Corollaire Si  $t$  désigne une indéterminée et si  $S$  est  $K[t]$ -reconnaissable, il existe  $C \in \mathbb{R}$  tel que  $\forall w \in X^+, \deg(S, w) \leq C |w|$ .

Preuve Il suffit de considérer sur  $K(t)$  la valeur absolue

$$|P/Q| = \exp(\deg(P) - \deg(Q)) \text{ et d'appliquer la proposition 5. } \square$$

La proposition suivante étend au cas des séries en plusieurs variables le critère d'Eisenstein (cf. Pólya et Szegő 1964 8. partie chap. 3).

Proposition 6 Soit  $K$  le corps des fractions de l'anneau  $A$ .

Si  $S$  est une série  $K$ -reconnaissable, il existe  $d \in A \setminus 0$  tels que la série  $\sum d^{1+|w|} (S, w) w$  soit  $A$ -reconnaissable.

Proposition 7 (Fliess 1974 th. 2.1.2) Soit  $K$  le corps des fractions de l'anneau principal  $A$ . Si  $S$  est une série  $K$ -reconnaissable à coefficients dans  $A$ ,  $S$  admet une représentation linéaire réduite à coefficients dans  $A$ .

## 4. SERIES RATIONNELLES

Les opérations rationnelles de  $K \langle\langle X \rangle\rangle$  sont : la somme, le produit (de Cauchy) et l'opération étoile. Une série  $S \in K \langle\langle X \rangle\rangle$  est dite *rationnelle* si elle appartient au plus petit sous-ensemble de  $K \langle\langle X \rangle\rangle$  contenant  $K \langle X \rangle$  et fermé pour les opérations rationnelles.

Théorème 1 (Kleene - Schützenberger) *Si  $X$  est fini, une série est rationnelle si et seulement si elle est reconnaissable.*

Pour une preuve, voir Schützenberger (1961 III) ou Eilenberg (1974 th. VII 5.1) ou encore Salomaa - Soittola (1977 th. II. 2. 3).

Nous parlerons dans ce travail indifféremment de séries rationnelles ou de séries reconnaissables (si l'alphabet est supposé fini).

## 5. LA GUERRE DES ETOILES

Au paragraphe 2, nous avons défini l'étoile d'une série propre (i.e. une série dont le terme constant est nul) par la formule

$$S^* = \sum_{n \geq 0} S^n$$

En fait, on pourrait définir  $S^*$  dès que la somme infinie ci-dessus converge. C'est ce que nous allons faire maintenant.

Proposition 1 *Soit  $S \in K \langle\langle X \rangle\rangle$  et  $a = (S, 1)$  son terme constant.*

*Alors  $\sum S^n$  converge si et seulement si la série  $\sum a^n$  converge dans  $K$  discret, i.e. si la suite  $\sum_{0 \leq i \leq n} a^i$  est stationnaire. On a alors*

$$\sum S^n = (a^* T)^+ a^* + a^* \quad \text{où} \quad T = \sum_{w \in X^+} (S, w) w \quad \text{est propre et}$$

$$a^* = \sum a^n.$$

Preuve Si  $\sum s^n$  converge dans  $K \ll X \gg$  il est clair que  $\sum a^n$  converge dans  $K$ . Nous établissons maintenant la réciproque, en nous remémorant la formule

$$(x+y)^* = (xy)^+ x^* + x^*$$

Soient  $p$  tel que  $1 = a + \dots + a^p = 1 + a + \dots + a^{p+1} = \dots = a^*$ ,

$N \geq 1$  et  $n = N + p(N+1)$

$$\begin{aligned} \text{Alors } \sum_{i=0}^n s^i &= \sum_{i=0}^n (a+T)^i \\ &= \sum_{k=0}^n \sum_{j_0+\dots+j_k \leq n-k} a^{j_0} T a^{j_1} \dots T a^{j_k} \\ &= \sum_{j=0}^n a^j + \sum_{k=1}^N \sum_{j_0+\dots+j_k \leq n-k} a^{j_0} T \dots T a^{j_k} + T_N \end{aligned}$$

où le premier terme vaut  $a^*$  et où le troisième vérifie  $\omega(T_N) \geq N+1$ , puisque  $T$  est propre.

Evaluons le second : nous montrons que

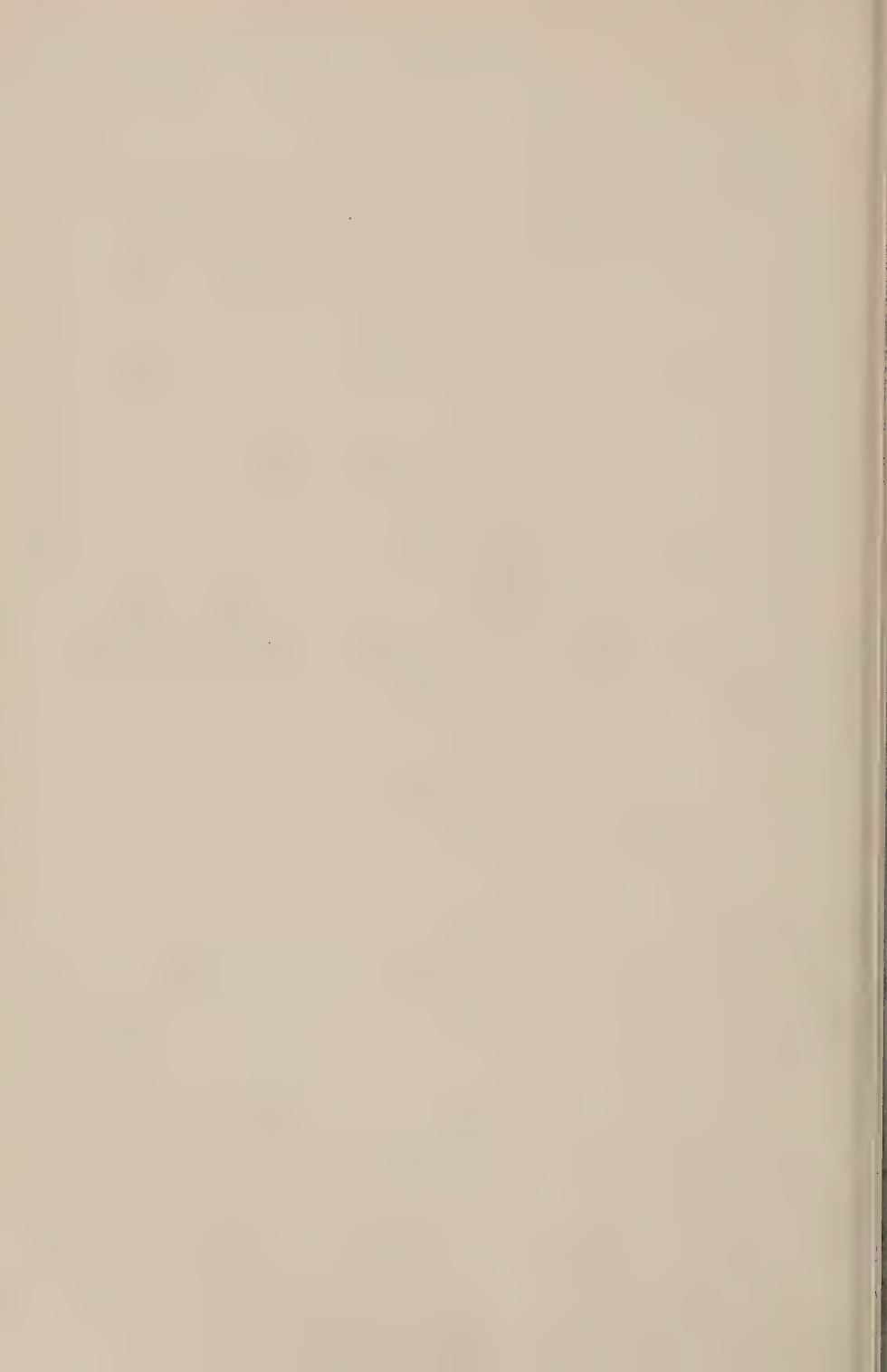
$$\sum_{j_0+\dots+j_k \leq h} a^{j_0} T \dots T a^{j_k} = \sum_{\substack{j_0+\dots+j_k \leq h \\ j_0, \dots, j_k \leq p}} a^{j_0} T \dots T a^{j_k}$$

Notons que si  $K$  est un anneau, alors  $a^{p+1} = 0$ , donc l'égalité ci-dessus est immédiate. Dans le cas général, nous raisonnons par récurrence sur  $k$ . Pour  $k=0$ , c'est clair car  $j \geq p$  implique  $1+a+\dots+a^j = 1+a+\dots+a^p$ . Soit  $k \geq 1$ .

Alors

$$\begin{aligned} \sum_{j_0+\dots+j_k \leq h} a^{j_0} T \dots T a^{j_k} &= \sum_{j_0+\dots+j_{k-1} \leq h} a^{j_0} T \dots T \sum_{0 \leq j \leq h-j_0-\dots-j_{k-1}} a^j \\ &= \sum_{\text{ibid.}} a^{j_0} T \dots T \sum_{\substack{\text{ibid} \\ j \leq p}} a^j \end{aligned}$$





$$\begin{aligned}
& \sum_{j_0 + \dots + j_k \leq h} a^{j_0} \dots a^{j_k} \\
&= \sum_{j \leq p, h} \left( \sum_{j_0 + \dots + j_{k-1} \leq h-j} a^{j_0} \dots a^{j_{k-1}} \right) a^j
\end{aligned}$$

qui est égal, par récurrence, à

$$\begin{aligned}
& \sum_{j \leq p, h} \left( \sum_{j_0 + \dots + j_{k-1} \leq h-j} a^{j_0} \dots a^{j_{k-1}} \right) a^j \\
& \quad j_0, \dots, j_{k-1} \leq p \\
&= \sum_{j_0 + \dots + j_k \leq h} a^{j_0} \dots a^{j_k} \quad \text{cqfd} \\
& \quad j_0, \dots, j_k \leq p
\end{aligned}$$

Notons encore que  $k \leq N$  et  $j_0, \dots, j_k \leq p$  implique

$j_0 + \dots + j_k \leq (k+1)p \leq p(N+1) = n - N \leq n - k$  donc le second terme de la somme ci-dessus est égale à

$$\sum_{k=1}^N \sum_{j_0, \dots, j_k \leq p} a^{j_0} \dots a^{j_k} = \sum_{k=1}^N (a^* T)^k a^*$$

Par suite

$$\sum_{0 \leq i \leq n} s^i = a^* + \left( \sum_{k=1}^N (a^* T)^k \right) a^* + T_N$$

et ceci pour tout  $N$ . Comme  $\lim_{N \rightarrow \infty} T_N = 0$ ,  $\sum s^n$ , converge et l'on a

$$\sum s^n = a^* + (a^* T)^+ a^* \quad \square$$

Corollaire Si  $\sum s^n$  converge et si  $S$  est rationnelle,  $\sum s^n$  l'est aussi

Remarque 1 Si le terme constant de  $S$  est nilpotent,  $\sum s^n$  converge.

La réciproque est vraie si  $K$  est un anneau.

Il est bien connu que si  $K$  est un anneau, alors une série  $S$  est inversible si et seulement si son terme constant est inversible dans  $K$ .

En effet, on se ramène toujours à  $(S, 1) = 1$  ; mais alors  $S = 1 - T$  où  $T$  est propre et

$$S^{-1} = \sum_{n \geq 0} T^{n1} = T^*.$$

On a donc clairement : l'inverse d'une série rationnelle inversible est encore une série rationnelle.

Toujours si  $K$  est un anneau, on peut faire une remarque analogue sur les éléments quasi-réguliers (au sens de Jacobson) : une série formelle  $S$  est quasi-régulière dans  $K \langle\langle X \rangle\rangle$  si et seulement si son terme constant l'est dans  $K$ . Si de plus,  $S$  est rationnelle, son quasi-inverse l'est aussi. Par ailleurs, le radical (de Jacobson) de  $K \langle\langle X \rangle\rangle$  est égal à l'ensemble des séries dont le terme constant est dans le radical de  $K$ . Si  $K$  est un corps, les séries quasi-régulières coïncident avec les séries propres, et le radical de  $K \langle\langle X \rangle\rangle$  est égal à l'idéal des séries propres.

## 6. MORPHISMES DE SERIES FORMELLES

Nous supposons, dans ce paragraphe, que les alphabets sont finis.

Définition 1 Soient  $K, L$  deux demianneaux et  $X, Y$  deux alphabets.

Une application

$$\varphi : K \langle\langle X \rangle\rangle \rightarrow L \langle\langle Y \rangle\rangle$$

est un *morphisme de séries formelles* si  $\varphi$  est un morphisme de demianneaux et si  $\varphi$  est uniformément continue.

Proposition 1 Si  $\varphi : K \langle\langle X \rangle\rangle \rightarrow L \langle\langle Y \rangle\rangle$  est un morphisme de demi-anneaux continu en 0, alors

(i) Pour toute lettre  $x \in X$  et tout élément  $k$  de  $K$ ,  $\varphi(x)$  commute à  $\varphi(k)$ .

(ii) Le sous-démigroupe de  $K$  engendré par les termes constants des séries  $\varphi(x)$ , où  $x$  parcourt  $X$ , est nilpotent.

Preuve (i) est clair puisque  $kx = xk$ .

(ii) Soit  $\psi : L \langle\langle Y \rangle\rangle \rightarrow L$  qui à une série formelle associe son terme constant ;  $\psi$  est un morphisme de demi-anneaux, qui est continu ( $L$  discret). Par suite

$$\psi \circ \varphi : K \langle\langle X \rangle\rangle \rightarrow L$$

est un morphisme de demi-anneaux continu en 0. Soit  $n \mapsto w_n$  une bijection  $\mathbb{N} \rightarrow X^*$ . On a  $\lim w_n = 0$ , puisque  $\omega(w_n) = |w_n|$  tend vers l'infini.

Par suite  $\lim \psi \circ \varphi(w_n) = 0$ , donc il existe un entier  $N'$  tel que  $n \geq N'$  implique  $\psi \circ \varphi(w_n) = 0$ . Il existe donc  $N$  tel que  $|w| \geq N$  implique  $w = w_n$  avec  $n \geq N'$ , donc  $\psi \circ \varphi(w) = 0$ .

Or  $\psi \circ \varphi(X^*)$  est précisément égal au sous-démigroupe de  $L$  engendré par les  $(\varphi(x), 1)$ ,  $x \in X$ , qui est donc nilpotent.  $\square$

Proposition 2 Soit  $\varphi : X \cup K \rightarrow L \langle\langle Y \rangle\rangle$  une application telle que la restriction de  $\varphi$  à  $K$  soit un morphisme de demi-anneaux vérifiant les conditions (i) et (ii) de la proposition précédente. Alors  $\varphi$  se prolonge d'une et d'une seule manière en un morphisme de séries formelles  $K \langle\langle X \rangle\rangle \rightarrow L \langle\langle Y \rangle\rangle$ .

Preuve Nous prolongeons d'abord  $\varphi$  en un morphisme de monoïdes  $X^* \rightarrow L \langle\langle Y \rangle\rangle$ , que nous notons encore  $\varphi$ . Puis nous prolongeons  $\varphi$  à  $K \langle\langle X \rangle\rangle$  par la formule

$$\varphi(p) = \sum_{w \in X^*} \varphi((p, w)) \varphi(w)$$

$\varphi$  est clairement un homomorphisme additif ; nous vérifions que  
 $\varphi(PQ) = \varphi(P) \varphi(Q)$ .

Notons d'abord que la condition (i) implique que pour tout mot  $w \in X^*$   
 et tout  $k \in K$ ,  $\varphi(w)$  commute à  $\varphi(k)$ . On a

$$\begin{aligned} (PQ, w) &= \sum_{uv=w} (P, u) (Q, v) \text{ donc} \\ \varphi(PQ) &= \sum_w \varphi \left( \sum_{uv=w} (P, u) (Q, v) \right) \varphi(w) \\ &= \sum_w \left( \sum_{uv=w} \varphi((P, u)) \varphi((Q, v)) \right) \varphi(w) \\ &= \sum_{u,v} \varphi((P, u)) \varphi((Q, v)) \varphi(u) \varphi(v) \\ &= \sum_{u,v} \varphi((P, u)) \varphi(u) \varphi((Q, v)) \varphi(v) \\ &= \left( \sum_u \varphi((P, u)) \varphi(u) \right) \left( \sum_v \varphi((Q, v)) \varphi(v) \right) \\ &= \varphi(P) \varphi(Q). \end{aligned}$$

Par suite  $\varphi: K \langle X \rangle \rightarrow L \langle\langle Y \rangle\rangle$  est un morphisme de demi-anneaux.

La condition (ii) implique l'existence d'un entier  $k \geq 1$  tel que pour  
 tout mot  $w$  de longueur au moins  $k$ ,  $(\varphi(w), 1) = 0$ . Nous vérifions que  
 pour tous mots  $w \in X^*$  et  $v \in Y^*$

$$|w| \geq (k-1)(|v|+1) + |v| \text{ implique } (\varphi(w), v) = 0.$$

Soit donc  $w = x_1 \dots x_n$ ,  $v = y_1 \dots y_p$  avec  $n \geq (k-1)(p+1) + p$ .

Alors

$$(\varphi(w), v) = \sum_{v_1 \dots v_n = v} (\varphi(x_1), v_1) \dots (\varphi(x_n), v_n)$$

L'inégalité ci-dessus et  $v_1 \dots v_n = v$  implique l'existence d'un  $i$  tel que  $v_{i+1} = \dots = v_{i+k} = 1$ . Par suite  $(\psi(w), v) = 0$ . Nous en déduisons que pour tous polynômes  $P$  et  $Q$

$$\omega(\psi(P), \psi(Q)) \geq \frac{\omega(P, Q)}{k} + 1 - k$$

En effet, soit  $v$  un mot de  $Y^*$  tel que

$$|v| < \frac{\omega(P, Q)}{k} + 1 - k$$

Alors  $(\psi(P), v) = \sum_w \psi(P, w) (\psi(w), v)$  et de même pour  $Q$ .

Si  $|w| > (k-1)(|v| + 1) + |v|$  alors  $(\psi(w), v) = 0$  donc la somme ci-dessus se réduit à

$$(\psi(P), v) = \sum_{|w| \leq (k-1)(|v| + 1) + |v|} \psi(P, w) (\psi(w), v)$$

et de même pour  $Q$ . Mais

$$|w| \leq (k-1)(|v| + 1) + |v| = k|v| + k - 1 \text{ implique } |w| < \omega(P, Q), \text{ donc}$$

$$(P, w) = (Q, w) \quad \text{d'où} \quad (\psi(P), v) = (\psi(Q), v).$$

D'où l'inégalité cherchée : elle implique que  $\psi: K \langle X \rangle \rightarrow L \langle\langle Y \rangle\rangle$  est uniformément continue.  $\psi$  se prolonge donc d'une et d'une seule manière en un morphisme uniformément continu  $K \langle X \rangle \rightarrow L \langle\langle Y \rangle\rangle$  puisque  $K \langle X \rangle$  est dense dans  $K \langle\langle X \rangle\rangle$ .  $\square$

Corollaire 1 (Berstel 1970) Si  $\psi$  est un morphisme de demianneaux

$K \langle\langle X \rangle\rangle \rightarrow L \langle\langle Y \rangle\rangle$  continu en 0, alors  $\psi$  est uniformément continue.

Remarque 1 Lorsque  $K$  est un anneau, l'uniforme continuité de  $\psi$  se ramène, par soustraction, à la continuité en 0, et le résultat est classique. Dans le cas général des demianneaux on ne peut plus soustraire, mais ceci est compensé, en quelque sorte, par l'ultramétrie de la topologie.

Corollaire 2 Si  $\varphi$  est un morphisme de séries formelles  $K \langle\langle X \rangle\rangle \rightarrow L \langle\langle Y \rangle\rangle$  tel que pour tout élément  $S$  de  $X \cup K$ ,  $\varphi(S)$  soit une série rationnelle, alors l'image par  $\varphi$  de toute série rationnelle est une série rationnelle.

Preuve Soit  $\mathcal{P}$  l'ensemble des séries  $S$  telles que  $\varphi(S)$  soit rationnelle ;  $\mathcal{P}$  contient  $X \cup K$ . Si  $S, T \in \mathcal{P}$ , alors  $\varphi(S + T) = \varphi(S) + \varphi(T)$  est rationnelle donc  $S + T \in \mathcal{P}$ ; de même  $\varphi(ST) = \varphi(S) \varphi(T)$  est rationnelle donc  $ST \in \mathcal{P}$ . Par suite  $\mathcal{P}$  contient  $K \langle\langle X \rangle\rangle$ .

Si  $S \in \mathcal{P}$  est une série propre, on a  $S^* = \sum S^n$  donc  $\varphi(S^*) = \sum \varphi(S^n) = \sum \varphi(S)^n$  puisque  $\varphi$  est continue. Comme  $\varphi(S)$  est rationnelle,  $\sum \varphi(S)^n$  l'est aussi (corollaire à la proposition 1 du §5), donc  $S \in \mathcal{P}$ . Par suite  $\mathcal{P}$  contient toutes les séries rationnelles.  $\square$

Définition 1 (Jacob 1975) Une représentation  $\mu : X^* \rightarrow K \langle\langle Y \rangle\rangle^{n \times n}$  est dite *régulée* s'il existe un entier  $k$  tel que  $\mu(X^k) \subset K^+ \langle\langle Y \rangle\rangle^{n \times n}$ , où  $K^+ \langle\langle Y \rangle\rangle$  désigne l'ensemble des séries propres. Elle est dite *rationnelle - régulée* si de plus toutes les entrées des matrices  $\mu w (w \in X^*)$  sont des séries rationnelles.

Corollaire 3 (Jacob) On suppose  $K$  commutatif. Soit  $\mu : X^* \rightarrow K \langle\langle Y \rangle\rangle^{n \times n}$  une représentation rationnelle régulée. Alors l'application

$$\begin{aligned} X^* &\longrightarrow K \langle\langle Y \rangle\rangle \\ w &\longmapsto (\mu w)_{1,n} \end{aligned}$$

se prolonge par linéarité et continuité à  $K \langle\langle X \rangle\rangle$  et l'image de toute série rationnelle est une série rationnelle.

Preuve Rappelons l'isomorphisme canonique

$$\begin{array}{ccc} K \langle\langle Y \rangle\rangle^{n \times n} & \longrightarrow & K \langle\langle Y \rangle\rangle^{n \times n} \\ m & \longmapsto & S \end{array}$$

où  $S$  est définie par  $(S, w) = ((m_{i,j}, w))_{1 \leq i, j \leq n}$

Si les  $m_{i,j}$  sont rationnelles, alors  $S$  est rationnelle : en effet, les séries

$$\sum_w (m_{i,j}, w) I_n w$$

sont alors des séries rationnelles ( $I_n$  est la matrice identité), donc aussi les séries

$$\sum_w (m_{i,j}, w) E_{i,j} w$$

( $E_{i,j}$  est la matrice élémentaire d'ordre  $i, j$ ) donc  $S$ , qui est la somme de ces séries, est rationnelle. Soit  $\varphi : X \rightarrow K^{n \times n} \langle\langle Y \rangle\rangle$  définie par  $\varphi(x) = \mu(x)$  (moyennant cet isomorphisme). La condition pour  $\mu$  d'être régulée correspond précisément à la condition (ii) de la proposition 1. La condition (i) est remplie si l'on pose  $\varphi(k) = k$ , pour tout  $k \in K$ , puisque  $K$  est commutatif.

Alors  $\varphi$  se prolonge en un morphisme de séries formelles

$K \langle\langle X \rangle\rangle \rightarrow K^{n \times n} \langle\langle Y \rangle\rangle$  (proposition 2) qui transforme toute série rationnelle en une série rationnelle (corollaire 2). Alors, pour toute série rationnelle  $S \in K \langle\langle X \rangle\rangle$ , la série  $\sum_w (S, w) (\mu w)_{1,n}$  est une série rationnelle (corollaire 4 à la proposition 1 du § 3).  $\square$

## 7. RELATIONS DE RECURRENCE LINEAIRES A DROITE

Rappelons qu'une partie  $P$  de  $X^*$  est dite *préfixielle* si elle si elle vérifie :

$$uv \in P \Rightarrow u \in P.$$

Un *code préfixe* est une partie  $C$  de  $X^*$  telle que

$$u, uv \in C \Rightarrow v = 1$$

Il y a bijection entre codes préfixes et parties préfixielles, de la manière suivante : à une partie préfixielle  $P$  on associe le code  $P \setminus X^*$  et à un code préfixe  $C$  on associe la partie préfixielle  $X^* \setminus C$  (voir aussi chapitre III § 4 exemple 1 (i)).

Nous disons qu'un code préfixe  $C$  est *complet* si pour tout mot  $w$

$$C \cap wX^* \neq \emptyset$$

La bijection ci-dessus induit, par restriction, une bijection entre parties préfixielles finies et code préfixes complets finis ; dans ce cas si  $P$  et  $C$  sont en bijection,  $P$  est aussi l'ensemble des mots qui sont facteur gauche d'un mot du code  $C$ .

Théorème 1 (Schützenberger 1961 III.B 1) Soit  $S$  une série formelle sur  $X$  à coefficients dans le corps commutatif  $K$ . Il existe une partie préfixielle de cardinal égal à rang  $(S)$  et des coefficients  $\alpha_{c,p}$  dans  $K$  ( $c \in C = P \setminus X^*$ ,  $p \in P$ ) tels que pour tout  $c \in C$  et tout mot  $w$

$$(S, cw) = \sum_{p \in P} \alpha_{c,p} (S, pw) \quad (*)$$

Remarque 1 Le théorème dit que si  $S$  est reconnaissable,  $P$  est fini, donc  $C$  est un code préfixe complet fini (Si  $S$  n'est pas reconnaissable, i.e. rang  $(S) = \infty$ , le théorème ne dit pas grand chose, puisqu'il suffit de prendre  $P = X^*$ , donc  $C = \emptyset \dots$ ).

Remarque 2 Si  $K$  est un anneau commutatif et  $X$  est fini, il existe aussi une version (plus faible) de ce résultat : si  $S \in K \langle\langle X \rangle\rangle$  est reconnaissable, il existe une partie préfixielle finie  $P$  et des coefficients  $\alpha_{c,p}$  tels qu'on ait la relation  $(*)$ .

En effet, soit  $(\lambda, \mu, \gamma)$  une représentation linéaire de  $S$  de dimension  $n$ . Soit  $L$  le sous-anneau de  $K$  engendré par les coefficients des matrices  $\lambda, \mu_{x(x \in X)}, \gamma$  :  $L$  est un anneau de type fini, donc  $L$

est noethérien. Alors  $L^n$  est un  $L$ -module noethérien ; si  $P$  est une partie de  $X^*$ , nous notons  $M(P)$  le sous-module de  $L^n$  engendré par les vecteurs  $\lambda \mu w$ ,  $w \in P$ . La famille des sous-modules  $M(P)$ , lorsque  $P$  parcourt l'ensemble des parties préfixielles finies de  $X^*$ , admet un élément maximal, soit  $M(P)$ . Soit  $C$  le code préfixe complet fini  $C = PX \setminus P$ . Si  $c \in C$ ,  $P \cup c$  est une partie préfixielle finie contenant  $P$  donc  $M(P) = M(P \cup c)$  et par suite il existe des  $\alpha_{c,p}$  dans  $L$  tels que

$$\lambda \mu c = \sum_{p \in P} \alpha_{c,p} \lambda \mu p$$

Alors, pour tout mot  $w$ , on obtient par multiplication à droite par  $\mu w \gamma$ :

$$(S, cw) = \sum_{p \in P} \alpha_{c,p} (S, p w) \quad \text{cqfd.}$$

## 8. SERIES RATIONNELLES REGULIERES

Nous supposons, dans ce paragraphe, que  $K$  est un corps

Définition 1 Nous disons qu'une série formelle  $S$  sur l'alphabet  $X$  à coefficients dans le corps commutatif  $K$  est *rationnelle régulière* si elle admet une représentation linéaire  $(\lambda, \mu, \gamma)$  telle que pour tout mot  $w$ ,  $\mu w$  est une matrice inversible.

Proposition 1 Les conditions suivantes sont équivalentes, pour une série rationnelle  $S$ .

- (i)  $S$  est rationnelle régulière
- (ii) Si  $(\lambda, \mu, \gamma)$  est une représentation linéaire réduite de  $S$ , pour tout mot  $w$ ,  $\mu w$  est une matrice inversible.
- (iii) Soit  $M = S \circ K \langle X \rangle$ : alors pour tout mot  $w$ , l'application  $T \mapsto T \circ w$  est un automorphisme de l'espace vectoriel  $M$ .

## 9. SERIES RATIONNELLES D'UNE VARIABLE

Soit  $K$  un corps commutatif.

Une série 
$$S = \sum_{n \geq 0} a_n x^n \in K[[x]]$$

est rationnelle si et seulement si elle est le développement en série d'une fraction rationnelle.

C'est encore équivalent à dire que la suite  $(a_n)$  vérifie une relation de récurrence linéaire, i.e. qu'il existe  $k \geq 1$  et des  $\alpha_1, \dots, \alpha_k$  dans  $K$  tels que

$$\forall n \geq 0, \quad a_{n+k} = \alpha_1 a_{n+k-1} + \dots + \alpha_k a_n$$

Si nous posons  $P = x^k - \alpha_1 x^{k-1} - \dots - \alpha_k$ , ceci s'écrit

$$P \circ S = 0$$

où  $\circ$  est l'opération de  $K[x]$  sur  $K[[x]]$  définie au §3 (en particulier  $x \circ S = \sum_{n \geq 1} a_{n-1} x^n$ ).

L'ensemble des polynômes  $P$  vérifiant  $P \circ S = 0$  est un idéal de  $K[x]$ . Nous appelons *polynôme minimal* de  $S$ , noté  $P_S$ , le générateur normalisé de cet idéal ; les *racines* de  $S$  sont les racines de  $P_S$  et leurs *multiplicités* sont leur multiplicité dans  $P_S$ . Le *rang* de  $S$  est égal au degré de  $P_S$  (cf. § 3).

La série  $S$  est rationnelle régulière (cf § 8) si et seulement si  $0$  n'est pas une racine de  $S$  ; c'est encore équivalent à dire qu'elle vérifie une relation de récurrence linéaire avec  $\alpha_k \neq 0$ , ou bien qu'elle est le développement en série d'une fraction rationnelle  $P/Q$  avec  $\deg(P) < \deg(Q)$ .

Lorsque  $K$  est de caractéristique nulle, la rationalité de  $S$  s'exprime aussi de la manière suivante : il existe des entiers naturels  $h$  et  $m$ , des éléments distincts  $\lambda_1, \dots, \lambda_m$  non nuls d'une extension

$L$  de  $K$ , des polynômes non nuls  $P_1(t), \dots, P_m(t)$  à coefficients dans  $L$  tels que

$$(1) \quad \forall n \geq h, a_n = \lambda_1^n P_1(n) + \dots + \lambda_m^n P_m(n)$$

Cette "expression" s'appelle le *polynôme exponentiel* de  $S$  : il est unique. Si  $h$  est choisi minimum, on a

$$P_S = x^h (x - \lambda_1)^{\deg(P_1)+1} \dots (x - \lambda_m)^{\deg(P_m)+1}$$

En particulier,  $S$  est régulière si et seulement si on a une égalité de la forme (1) pour tout  $n \geq 0$ .

Pour toutes ces considérations voir Pisot (1959) et Polya et Szegő (1964).

L'existence et l'unicité du polynôme exponentiel, ainsi que son rapport avec le produit de Hadamard, peut se formuler de la manière suivante.

Proposition 1 Soit  $K$  un corps algébriquement clos de caractéristique nulle,  $G$  le groupe multiplicatif  $K \setminus 0$  et  $t$  une indéterminée. Il y a isomorphisme entre l'algèbre du groupe  $G$  sur l'anneau  $K[t]$ , et l'algèbre de Hadamard des séries rationnelles régulières, de la manière suivante :

à  $E = \sum_{\lambda \in G} P_\lambda(t) \lambda$  on associe la série  $\sum a_n x^n$  avec

$$\forall n \geq 0, a_n = \sum_{\lambda \in G} P_\lambda(n) \lambda^n$$

(cette dernière somme est effectuée dans  $K$ )

Preuve Le fait que cette application est une bijection vient d'être vu.

Appelons  $\varphi$  cette application, et soit  $E = \sum P_\lambda(t) \lambda$ ,  $F = \sum Q_\lambda(t) \lambda$

Alors

$$\begin{aligned}
 \Psi(E + F)_n &= \sum_{\lambda \in G} (P_\lambda + Q_\lambda)(n) \lambda^n \\
 &= \sum P_\lambda(n) \lambda^n + \sum Q_\lambda(n) \lambda^n = \Psi(E)_n + \Psi(F)_n \\
 \Psi(E F)_n &= \sum_{\lambda \in G} \lambda^n \left( \sum_{\lambda = \mu \nu} P_\mu Q_\nu \right)(n) \\
 &= \sum P_\mu(n) Q_\nu(n) \mu^n \nu^n \\
 &= \left( \sum_\mu P_\mu(n) \mu^n \right) \left( \sum_\nu Q_\nu(n) \nu^n \right) = \Psi(E)_n \Psi(F)_n. \quad \square
 \end{aligned}$$

En caractéristique non nulle, ce résultat n'est plus vrai. Nous avons quand même la proposition suivante (évidente, mais cependant utile).

Proposition 2 Soit  $K$  un corps commutatif et  $G$  le groupe multiplicatif  $K \setminus 0$ . L'application de la  $K$ -algèbre du groupe  $G$  dans l'algèbre de Hadamard des séries rationnelles régulières, définie par

$$\sum_{\lambda \in G} P_\lambda \lambda \longmapsto \sum_{n \geq 0} a_n x^n$$

où  $a_n = \sum P_\lambda \lambda^n$   
est un homomorphisme injectif.

Preuve Il suffit de vérifier que cette application est injective. Mais si  $\lambda_1, \dots, \lambda_m \in K \setminus 0$  sont distincts deux à deux et si  $P_1, \dots, P_m \in K$ , les relations

$$\forall n \geq 0, \quad \sum_{1 \leq i \leq m} P_i \lambda_i^n = 0$$

impliquent  $P_1 = \dots = P_m = 0$ . En effet, on a alors

$$\begin{aligned}
 P_1 + \dots + P_m &= 0 \\
 P_1 \lambda_1 + \dots + P_m \lambda_m &= 0 \\
 \vdots \\
 P_1 \lambda_1^{m-1} + \dots + P_m \lambda_m^{m-1} &= 0
 \end{aligned}$$

ce qui est un système de Cramer en les  $P_i$  qui sont donc tous nuls.  $\square$

Les considérations qui suivent sont un peu techniques. Mais elles nous seront fort utiles pour tout ce qui concerne, dans la suite de ce travail, les séries rationnelles d'une variable.

Définition 1 Soient  $S_0, \dots, S_{N-1} \in K[[x]]$ , avec  $S_i = \sum_{n \geq 0} a_n^i x^n$ .

L'emboîtement des séries  $S_0, \dots, S_{N-1}$  (dans cet ordre) est la série  $S = \sum a_n x^n$  définie par : pour tout  $n$ ,  $a_n$  est égal à  $a_q^i$  si  $q$  est le quotient de la division euclidienne de  $n$  par  $N$  et  $i$  le reste, i.e. pour tout  $n \geq 0$  et tout  $i$ ,  $0 \leq i < N$ , on a :  $a_{i+nN} = a_n^i$ .

Exemple 1 L'emboîtement de  $S_0$  et  $S_1$  est défini par  $a_n = a_k^0$  si  $n = 2k$  et  $a_n = a_k^1$  si  $n = 2k + 1$ . La suite  $(a_n)$  est alors la suite

$$a_0^0, a_0^1, a_1^0, a_1^1, a_2^0, a_2^1, a_3^0, \dots$$

Définition 2 (i) Soit  $S \in K[[x]]$  une série rationnelle.  $S$  est dite *normale* si les racines de  $S$  engendrent un sous-groupe multiplicatif (abélien) libre et si de plus, lorsque  $K$  est de caractéristique non nulle, elles sont toutes de multiplicité égale à un.

(ii) Le couple  $(S, T)$  est dit *normal* si chacune des séries  $S$  et  $T$  est rationnelle normale et si de plus le groupe engendré par les racines de  $S$  et celles de  $T$  est libre.

Exemple 2 Si  $K = \mathbb{Q}$ , les séries  $\sum (2^n + 3^n)x^n$  et  $\sum (1+2^n)x^n$  sont normales. La série  $\sum (-1)^n x^n$  n'est pas normale, mais elle est égale à l'emboîtement des deux séries normales  $\sum x^n$  et  $-\sum x^{2n}$ .

Remarque 1 Quelle que soit la caractéristique de  $K$ , une série rationnelle régulière  $S$  a toutes ses multiplicités égales à un si et seulement s'il existe, dans une extension de  $K$ , des éléments  $P_1, \dots, P_m, \lambda_1, \dots, \lambda_m$  telles que

$$S = \sum_{n \geq 0} (P_1 \lambda_1^n + \dots + P_m \lambda_m^n) x^n$$

Pour s'en convaincre, il suffit de considérer la fraction rationnelle dont  $S$  est le développement et de la décomposer en éléments simples.

Pour alléger les notations, nous posons la définition suivante.

Définition 3 Soit  $P = \prod (x - \lambda_i)^{n_i} \in K[x]$  et  $N$  un entier. Nous notons  $P^{(N)}$  le polynôme  $\prod (x - \lambda_i)^{n_i N}$ .

Remarque 2 Les coefficients de  $P^{(N)}$  sont dans le corps  $K_1$  engendré par les coefficients de  $P$ . Pour le voir, on peut par exemple associer à  $P$  une matrice  $A \in K_1^{n \times n}$  dont les coefficients sont dans  $K_1$  et dont le polynôme caractéristique est égal à  $P$ . Alors  $P^{(N)}$  est le polynôme caractéristique de  $A^N$  et ses coefficients sont dans  $K_1$ .

La proposition qui suit est la plus importante de ce paragraphe. Elle nous permettra, plus tard d'emprunter des raccourcis agréables.

Proposition 3 Etant données deux séries rationnelles régulières  $S$  et  $T$  dans  $K[[x]]$  il existe un entier  $N$  et des séries rationnelles  $S_0, \dots, S_{N-1}, T_0, \dots, T_{N-1}$  telles que pour tout  $k$  le couple  $(S_k, T_k)$  soit normal et que  $S$  (resp.  $T$ ) soit égal à l'emboîtement des séries  $S_0, \dots, S_{N-1}$  (resp.  $T_0, \dots, T_{N-1}$ ). De manière précise, si  $P$  et  $Q$  sont des polynômes tels que  $PoS = 0$  et  $QoT = 0$ , on peut choisir  $N$  ne dépendant que des degrés de  $P$  et de  $Q$  et du corps engendré par les coefficients de  $P$  et de  $Q$  et tel que  $P^{(N)} \circ S_k = 0$  et  $Q^{(N)} \circ T_k = 0$ , pour tout  $k$ , et que le groupe engendré par les racines non nulles de  $P^{(N)}$  et de  $Q^{(N)}$  soit (abélien) libre.

Nous avons besoin de plusieurs lemmes.

Lemme 1 Soit  $K_1$  un corps de type fini (i.e. une extension de son sous-corps premier par un nombre fini d'éléments) et  $M$  un entier. Il n'y a qu'un nombre fini de racines de l'unité qui sont algébriques sur  $K_1$  de degré  $\leq M$ .

Pour une preuve voir par exemple Reutenauer (1977, appendice) ; ce résultat se trouve implicitement dans Kaplansky (1969 p. 104).

Lemme 2 Soient  $S, S_0, \dots, S_{N-1}$  des séries rationnelles et  $P$  un polynôme tels que  $PS = 0$  et que  $S$  est égal à l'emboîtement des séries  $S_0, \dots, S_{N-1}$ . Alors, pour tout  $k$ , on a  $P^{(N)} \circ S_k = 0$ .

Preuve Il existe une matrice  $A \in K^{n \times n}$ , des matrices  $\lambda \in K^{l \times n}$  et  $\gamma \in K^{n \times 1}$  telles que

$$\forall n, a_n = \lambda A^n \gamma$$

(où  $S = \sum a_n x^n$ ) et que le polynôme caractéristique de  $A$  soit égal à  $P$  (on peut prendre pour  $A$  la matrice "compagnon" de  $P$ ). Alors pour tout  $k$ ,  $0 \leq k \leq N-1$ , on a

$$S_k = \sum_{n \geq 0} \lambda A^k (A^N)^n \gamma x^n$$

Or, le polynôme caractéristique de  $A^N$  est égal à  $P^{(N)}$ , ce qui permet de conclure.  $\square$

Lemme 3 On suppose que  $K$  est un corps de caractéristique non nulle. Soient  $S$  et  $T$  des séries rationnelles régulières et  $P$  et  $Q$  deux polynômes tels que  $PS = 0$  et  $Q \circ T = 0$ . Il existe un entier  $N$  ne dépendant que des degrés de  $P$  et  $Q$ , et des séries rationnelles  $S_0, \dots, S_{N-1}, T_0, \dots, T_{N-1}$ , dont les racines sont des puissances  $N^{\text{ème}}$

des racines de  $P$  et de  $Q$  et dont les multiplicités sont égales à  $m_i$ , telles que  $S$  (resp.  $T$ ) est égale à l'emboîtement des séries  $S_0, \dots, S_{N-1}$  (resp.  $T_0, \dots, T_{N-1}$ ).

Preuve Elle est analogue à celle de l'existence du polynôme exponentiel en caractéristique nulle. Comme  $S$  et  $T$  sont régulières, il existe des polynômes  $A$  et  $B$  dans  $K[x]$  tels que  $\deg(A) < \deg(P)$ ,  $\deg(B) < \deg(Q)$  et que

$$S = \frac{A}{\prod (1 - \lambda_i x)^{n_i}}, \quad T = \frac{B}{\prod (1 - \mu_j x)^{m_j}}$$

où nous avons posé  $P = \prod (x - \lambda_i)^{n_i}$  et  $Q = \prod (x - \mu_j)^{m_j}$ .

Décomposons ces fractions rationnelles en éléments simples.

$$S = \sum_i \sum_{1 \leq r \leq n_i} \frac{a_{i,r}}{(1 - \lambda_i x)^r}, \quad T = \sum_j \sum_{1 \leq s \leq m_j} \frac{b_{j,s}}{(1 - \mu_j x)^s}$$

$$\text{Or, } \frac{1}{(1 - \nu x)^t} = \sum_{n \geq 0} \nu^n \binom{n+t-1}{t-1} x^n, \text{ où le coefficient } \binom{n+t-1}{t-1}$$

doit être interprété comme la valeur, modulo  $p$  (la caractéristique de  $K$ ) de l'entier  $\binom{n+t-1}{t-1}$ . Mais la suite d'entiers  $\alpha_n = \binom{n+t-1}{t-1}$  est périodique modulo  $p$ , et cette période peut être majorée en fonction de  $t$ . Il existe donc un entier  $N$ , ne dépendant que du degré de  $P$  et du degré de  $Q$ , qui est une période commune pour toutes les suites  $\binom{n+t-1}{t-1}$ ,  $t \leq \sup \{n_i, m_j\}$ . Pour conclure nous appliquons la remarque 1 et le lemme 2.  $\square$

Preuve de la proposition 3

$$P = \prod_i (x - \lambda_i)^{n_i} \text{ et } Q = \prod_j (x - \mu_j)^{m_j}.$$

Soit  $K_1$  le sous-corps de  $K$  engendré par les coefficients de  $P$  et  $Q$ . Il existe un entier  $M$ , ne dépendant que des degrés de  $P$  et de  $Q$ , tel que l'extension de  $K_1$  par les racines  $P$  et  $Q$  ait un degré sur  $K_1$  majoré par  $M$ . Par suite, d'après le lemme 1, il existe un entier  $N'$  tel que l'ordre de toute racine de l'unité contenue dans  $L$  divise  $N'$ . Le sous-groupe multiplicatif de  $L$  engendré par les  $\lambda_i$  et les  $\mu_j$  est de type fini, donc il est isomorphe au produit  $G \times F$  d'un groupe abélien libre par un groupe fini  $F$ . Tout élément de  $F$  est d'ordre fini, donc c'est une racine de l'unité contenue dans  $L$  et son ordre divise  $N'$ . Par suite, le sous-groupe de  $L$  engendré par les  $\lambda_i^{N'}$  et les  $\mu_j^{N'}$  est contenu dans  $G$  et il est donc (abélien) libre. Soient  $S_0, \dots, S_{N'-1}$ ,  $T_0, \dots, T_{N'-1}$  les séries telles que  $S$  est égale à l'emboîtement de  $S_0, \dots, S_{N'-1}$  et  $T$  à celui de  $T_0, \dots, T_{N'-1}$ . D'après le lemme 2, le polynôme minimal des  $S_k$  (resp. des  $T_k$ ) divise  $\prod (x - \lambda_i^{N'})^{n_i}$  (resp.  $\prod (x - \mu_j^{N'})^{m_j}$ ). Nous pouvons donc conclure si la caractéristique de  $K$  est nulle, et posons  $N' = N$ . Si elle n'est pas nulle, nous appliquons le lemme 3, pour obtenir chaque série  $S_k$  et  $T_k$  comme un emboîtement de séries normales (cf. remarque 1) et ceci permet de conclure.  $\square$

Proposition 4. *Soit  $S$  une série rationnelle. Il existe une série rationnelle régulière  $T$  telle que  $S - T$  soit un polynôme dont le degré est strictement inférieur à la multiplicité de 0 comme racine de  $S$  (donc inférieur au rang de  $S$ ).*

Preuve. Soit  $P = x^q Q$  le polynôme minimal de  $S$ , où  $q$  est la multiplicité de 0 dans  $P$ . Comme  $P \circ S = 0$  on a  $x^q \circ (Q \circ S) = 0$  donc  $Q \circ S$  est un polynôme de degré au plus  $q - 1$ . Considérons l'application linéaire  $R \mapsto Q \circ R$  de  $K[x]$  dans  $K[x]$  : on a  $\deg(Q \circ R) = \deg(R)$

puisque  $Q(0) \neq 0$ . Par suite, cette application est un automorphisme et il existe  $R \in K[x]$  tel que  $Q \circ R = Q \circ S$  et  $\deg(R) \leq q-1$ . Soit  $T = S - R$ . Alors  $Q \circ T = Q \circ S - Q \circ R = 0$  et  $T$  est régulière.  $\square$

Proposition 5 *Si  $S$  est une série rationnelle régulière égale à un polynôme, alors  $S = 0$ .*

Preuve Soit  $S = \sum a_n x^n$ . Il existe  $k \geq 1$  et des  $\alpha_1, \dots, \alpha_k$  tels que  $\alpha_k \neq 0$  ( $S$  régulière) et  $\forall n, a_{n+k} = \alpha_1 a_{n+k-1} + \dots + \alpha_k a_n$ .

Si  $S \neq 0$ , soit  $n$  le plus grand entier tel que  $a_n \neq 0$  (il existe, puisque  $S$  est un polynôme). Alors  $a_{n+1} = \dots = a_{n+k-1} = a_{n+k} = 0$  et  $\alpha_k \neq 0$  donc  $a_n = 0$ , ce qui est absurde.  $\square$

## CHAPITRE II - ALGÈBRES SYNTACTIQUES

-----

Dans ce chapitre nous introduisons notre outil principal pour l'étude des séries rationnelles : l'algèbre syntactique. C'est un objet tout-à-fait analogue au monoïde syntactique d'un langage : la notion de congruence du monoïde libre est remplacée par celle d'idéal de l'algèbre libre et l'algèbre syntactique d'une série formelle est le quotient le plus petit de l'algèbre libre qui reconnaît cette série. Comme pour les monoïdes syntactiques, l'algèbre syntactique d'une série reflète dans sa structure algébrique des propriétés combinatoires de la série. De la même manière que le monoïde syntactique d'un langage s'identifie au monoïde de transitions de son automate minimal, l'algèbre syntactique d'une série formelle s'identifie à l'algèbre des endomorphismes de son module sériel réduit, tel que l'a défini Fliess (§ 2). Par ailleurs, le monoïde syntactique d'un langage s'identifie à l'image du monoïde libre dans l'algèbre syntactique de sa série caractéristique, et celle-ci est quotient de l'algèbre du monoïde syntactique de ce langage (§ 3). Au dernier paragraphe, nous vérifions par des méthodes standards, comment réagit l'algèbre syntactique à l'extension de l'anneau des scalaires.

Dans ce chapitre  $K$  désigne un anneau commutatif unitaire et  $X$  un alphabet non nécessairement fini. Les  $K$ -algèbres considérées ici seront associatives et munies d'un élément neutre. Les homomorphismes de  $K$ -algèbres conserveront l'élément neutre et une sous-algèbre d'une algèbre aura toujours même élément neutre que celle-ci. Nous dirons souvent idéal pour idéal bilatère et algèbre pour  $K$ -algèbre.

1 - REPRESENTATION D'UNE SERIE FORMELLE.

Rappelons que  $K\langle X \rangle$  s'identifie au  $K$ -module dual de  $K[X]$  : chaque série formelle  $S \in K\langle X \rangle$  définit une forme linéaire

$$K\langle X \rangle \longrightarrow K$$

$$P \longmapsto (S, P)$$

avec

$$(S, P) = \sum_{w \in X^*} (S, w) (P, w)$$

somme dont seulement un nombre fini de termes sont non nuls puisque  $P$  est un polynôme.

Nous confondrons dans la suite, une série formelle  $S$  et la forme linéaire qu'elle définit. En particulier nous noterons  $\text{Ker } S$  le noyau de  $S$ .

$$\text{Ker } S = \{ P \in K\langle X \rangle \mid (S, P) = 0 \}$$

Définition 1 - Une  $K$ -représentation de  $S$  est un triplet  $(\mathcal{M}, \mu, \varphi)$  où  $\mathcal{M}$  est une  $K$ -algèbre,  $\mu$  un homomorphisme de  $K$ -algèbres  $K\langle X \rangle \rightarrow \mathcal{M}$  et  $\varphi$  une forme linéaire sur  $\mathcal{M}$  tel que le diagramme suivant soit commutatif :

$$\begin{array}{ccc} K\langle X \rangle & \xrightarrow{S} & K \\ \mu \searrow & & \nearrow \varphi \\ & \mathcal{M} & \end{array}$$

La représentation est dite *finie* (resp. *surjective*) si  $\mathcal{M}$  est un  $K$ -module de type fini (resp. si  $\mu$  est surjectif).

Remarque 1 - Comme  $X^*$  est une base de  $K\langle X \rangle$ , la commutativité du diagramme ci-dessus équivaut à :  $\forall w \in X^*, (S, w) = \varphi \circ \mu(w)$ .

Exemple 1. Une représentation de la série  $S$  est le triplet

$$(K\langle X \rangle, \text{id}, S)$$

où  $\text{id} : K\langle X \rangle \rightarrow K\langle X \rangle$  est l'identité.

Nous allons voir que parmi les représentations de  $S$  il en existe une qui possède des propriétés remarquables : elle sera appelée la *représentation minimale*.

Lemme 1. Soit  $M$  une  $K$ -algèbre et  $V$  un sous- $K$ -module de  $M$ . Il existe, parmi les idéaux contenus dans  $V$ , un plus grand idéal. Il est égal à

$$\{ m \in M \mid \forall m_1, m_2 \in M, m_1 m m_2 \in V \}$$

Preuve. L'ensemble des idéaux contenus dans  $V$  est non vide puisqu'il contient  $0$ . La somme de tous ces idéaux est clairement un idéal, et c'est le plus grand idéal contenu dans  $V$ . Soit  $J_V$  cet idéal et

$$J = \{ m \in M \mid \forall m_1, m_2 \in M, m_1 m m_2 \in V \}$$

-  $J$  est un sous-groupe de  $M$  : en effet, si  $m, m' \in J$ ,  $m_1, m_2 \in M$ , on a

$$m_1 (m + m') m_2 = m_1 m m_2 + m_1 m' m_2 \in V$$

puisque  $V$  est un sous-groupe de  $M$ .

-  $J$  est un idéal : en effet, si  $m \in J$  et  $m', m'' \in M$ , on a pour tous  $m_1, m_2 \in M$

$$m_1 (m' m m'') m_2 = (m_1 m') m (m'' m_2) \in V$$

donc

$$m' m m'' \in J.$$

-  $J$  contient  $J_V$  : en effet, si  $m \in J_V$  et  $m_1, m_2 \in M$ , on a  $m_1 m m_2 \in J_V$  car  $J_V$  est un idéal. Or,  $J_V \subset V$  donc  $m_1 m m_2 \in V$ . Par suite  $m \in J$ .

-  $J$  est contenu dans  $V$  : en effet si  $m \in J$ ,  $m = 1 m 1 \in V$ .

Par conséquent  $J$  est égal à  $J_V$ .  $\square$

Nous pouvons maintenant poser la

Définition 2. L'idéal syntactique de la série formelle  $S$  est le plus grand idéal de  $K\langle X \rangle$  contenu dans  $\text{Ker } S$ . On le note  $\mathcal{I}_S$ . L'algèbre syntactique de  $S$  est l'algèbre :

$$\mathcal{M}_S = K\langle X \rangle / \mathcal{I}_S.$$

Lemme 2. On a les relations

$$\begin{aligned} \mathcal{I}_S &= \{ P \in K\langle X \rangle \mid \forall Q, R \in K\langle X \rangle \quad (S, QPR) = 0 \} \\ &= \{ P \in K\langle X \rangle \mid \forall u, v \in X^* \quad (S, uPv) = 0 \} \end{aligned}$$

Preuve. La première relation découle du lemme 1. Pour la seconde on remarque que  $X^*$  est une base du  $K$ -module  $K\langle X \rangle$  :

Soit  $P \in K\langle X \rangle$  tel que pour tous  $u, v \in X^*$ ,  $(S, uPv) = 0$ . Alors pour tous  $Q, R \in K\langle X \rangle$

$$\begin{aligned} (S, QPR) &= (S, \left[ \sum_{u \in X^*} (Q, u) u \right] P \left[ \sum_{v \in X^*} (R, v) v \right]) \\ &= \sum_{u, v \in X^*} (Q, u) (R, v) (S, uPv) = 0 \end{aligned}$$

par linéarité de  $S$ .  $\square$

Remarque 2. Avec les notations du § 3 du chapitre 1, le lemme 2 exprime que  $\mathcal{I}_S$  est égal à l'orthogonal du sous-module de  $K\langle X \rangle$  engendré par les séries (les formes linéaires)

$$u \circ S \circ v, \quad u, v \in X^*.$$

Nous notons  $\mu_S$  l'homomorphisme canonique

$$\mu_S : K\langle X \rangle \rightarrow K\langle X \rangle / \mathcal{I}_S = \mathcal{M}_S$$

Comme  $\mathfrak{I}_S \subset \text{Ker } S$ ,  $S$  définit sur  $\mathcal{M}_S$  une forme linéaire

$$\varphi_S : \mathcal{M}_S \rightarrow K$$

de telle manière que le diagramme suivant soit commutatif :

$$\begin{array}{ccc} K \langle X \rangle & \xrightarrow{S} & K \\ \mu_S \searrow & & \nearrow \varphi_S \\ & \mathcal{M}_S & \end{array}$$

Autrement dit, le triplet

$$(\mathcal{M}_S, \mu_S, \varphi_S)$$

est une représentation de  $S$ , qui est clairement surjective. Cette représentation est appelée la *représentation minimale* de  $S$ , et possède la propriété fondamentale (mais néanmoins facile à établir) suivante.

Théorème 1. Soit  $(\mathcal{M}, \mu, \varphi)$  une représentation surjective de  $S$ . Il existe un homomorphisme d'algèbres

$$\nu : \mathcal{M} \rightarrow \mathcal{M}_S$$

(nécessairement unique et surjectif) tel que le diagramme suivant soit commutatif :

$$\begin{array}{ccc} & K \langle X \rangle & \\ \mu \swarrow & & \searrow \mu_S \\ \mathcal{M} & \xrightarrow{\nu} & \mathcal{M}_S \end{array}$$

Preuve. On a par définition  $S = \varphi \circ \mu$ . Par suite l'idéal  $\text{Ker } \mu$  est contenu dans  $\text{Ker } S$ . Par définition de  $\mathfrak{I}_S$  on a  $\text{Ker } \mu \subset \mathfrak{I}_S$  et l'existence de  $\nu$ , ainsi que son unicité, découlent de la surjectivité de  $\mu$ ; celle-ci implique aussi celle de  $\nu$ .  $\square$

Définition 3. (i) Nous disons qu'une algèbre  $\mathcal{M}$  reconnaît la série formelle  $S$  s'il existe une représentation de  $S$  de la forme  $(\mathcal{M}, \mu, \varphi)$ .

(ii) Soient  $\mathcal{M}_1, \mathcal{M}_2$  deux algèbres. Nous disons que  $\mathcal{M}_1$  divise  $\mathcal{M}_2$  s'il existe une sous-algèbre de  $\mathcal{M}_2$  à un quotient duquel  $\mathcal{M}_1$  est isomorphe.

Notation :  $\mathcal{M}_1 < \mathcal{M}_2$

Corollaire. Si  $\mathcal{M}$  reconnaît  $S$ ,  $\mathcal{M}_S$  divise  $\mathcal{M}$ .

Preuve. Par définition,  $S$  admet une représentation de la forme  $(\mathcal{M}, \mu, \varphi)$

Soit  $\mathcal{M}' = \mu(K\langle X \rangle)$  et  $\varphi'$  la restriction de  $\varphi$  à  $\mathcal{M}$ . Alors

$(\mathcal{M}', \mu, \varphi')$  est une représentation surjective de  $S$ . D'après le théorème 1,  $\mathcal{M}_S$  est quotient de  $\mathcal{M}'$  donc  $\mathcal{M}_S$  divise  $\mathcal{M}$ .  $\square$

Définition 4. Nous disons qu'une algèbre  $\mathcal{M}$  est syntactique s'il existe un alphabet  $X$  et une série formelle  $S \in K\langle\langle X \rangle\rangle$  tels que  $\mathcal{M} = \mathcal{M}_S$ .

Ici, il faut remarquer qu'il existe des algèbres qui ne sont pas syntactiques (voir l'exemple 2 ci-dessous).

Lemme 3. Soit  $S \in K\langle\langle X \rangle\rangle$  et  $\mathcal{J}$  un idéal de  $\mathcal{M}_S$  contenu dans  $\text{Ker } \varphi_S$ .

Alors  $\mathcal{J} = 0$ .

Preuve. On a  $\mathcal{J} \subset \text{Ker } \varphi_S$ , donc l'idéal  $\mu_S^{-1}(\mathcal{J})$  est contenu dans

$\mu_S^{-1}(\text{Ker } \varphi_S) = \text{Ker } S$ . Par définition de  $\mathcal{J}_S$  on a  $\mu_S^{-1}(\mathcal{J}) \subset \mathcal{J}_S$ , donc

$\mathcal{J} = \mu_S(\mu_S^{-1}(\mathcal{J})) \subset \mu_S(\mathcal{J}_S) = 0$ .  $\square$

Proposition 1. Une algèbre non nulle est syntactique si et seulement si elle contient un hyperplan (i.e. le noyau d'une forme linéaire non nulle) ne contenant aucun idéal non nul.

Autrement dit, une algèbre non nulle n'est pas syntactique si et seulement si tout hyperplan contient un idéal non nul.

Preuve. Soit  $\mathcal{M}$  une algèbre syntactique non nulle :  $\mathcal{M} = \mathcal{M}_S$  pour une série formelle  $S \in K \langle\langle X \rangle\rangle$ .  $S$  est non nulle (sinon  $\mathcal{I}_S = K \langle X \rangle$  et  $\mathcal{M}_S = 0$ ) donc  $\varphi_S \neq 0$  et  $\text{Ker } \varphi_S$  est un hyperplan de  $\mathcal{M}_S$ . Si  $\mathcal{I}$  est un idéal de contenu dans  $\text{Ker } \varphi_S$ , alors  $\mathcal{I} = 0$  d'après le lemme 3.

Soit  $\mathcal{M}$  une algèbre et  $H$  un hyperplan de  $\mathcal{M}$  ne contenant aucun idéal non nul. On a  $H = \text{Ker } \varphi$  pour une forme linéaire  $\varphi$  non nulle sur  $\mathcal{M}$ . Soit  $X$  un alphabet tel qu'il existe un homomorphisme surjectif d'algèbres

$$\mu : K \langle X \rangle \rightarrow \mathcal{M}$$

Soit  $S$  la série formelle sur  $X$  définie par

$$S = \varphi \circ \mu.$$

On a  $\text{Ker } \mu \subset \text{Ker } S$  donc  $\text{Ker } \mu \subset \mathcal{I}_S$ . De plus, si  $P \in \mathcal{I}_S$ , on a  $\varphi \circ \mu(P) = (S, P) = 0$  donc  $\mu(\mathcal{I}_S) \subset \text{Ker } \varphi$ . Par suite  $\mu(\mathcal{I}_S)$  est un idéal de  $\mathcal{M}$  contenu dans  $\text{Ker } \varphi$  et par hypothèse  $\mu(\mathcal{I}_S) = 0$ , donc  $\mathcal{I}_S \subset \text{Ker } \mu$ . D'où  $\mathcal{I}_S = \text{Ker } \mu$  et  $\mathcal{M} = \mathcal{M}_S$ .  $\square$

Exemple 2. Un exemple d'algèbre non syntactique est le suivant :

Soit  $\mathcal{M} = K.1 \oplus K.x \oplus K.y$ ,

où la multiplication est définie par

$$x^2 = xy = yx = y^2 = 0.$$

Soit  $\varphi$  une forme linéaire sur  $\mathcal{M}$ . Il existe  $m = ax + by \in \text{Ker } \varphi$  avec  $m \neq 0$  (en effet, si  $\varphi(x) = \varphi(y) = 0$ , c'est clair, sinon l'on prend  $m = \varphi(y)x - \varphi(x)y$ ). L'idéal engendré par  $m$  est  $K.m$  et il est contenu dans  $\text{Ker } \varphi$ .

Proposition 2. Soient  $\mathcal{M}_1, \dots, \mathcal{M}_n$  des algèbres syntactiques. Alors  $\mathcal{M} = \prod \mathcal{M}_i$  est syntactique.

Preuve. Soit  $\varphi_i$  une forme linéaire sur  $\mathcal{M}_i$  tel que  $\text{Ker } \varphi_i$  ne contient aucun idéal non nul,  $i = 1, \dots, n$ . Soit  $\varphi$  la forme linéaire sur  $\mathcal{M}$  définie par  $\varphi = \prod \varphi_i$ . Soit  $\mathcal{J}$  un idéal contenu dans  $\text{Ker } \varphi$  et  $m = \sum m_i \in \mathcal{J}$ . Alors pour tout  $i$ ,  $m_i \in \text{Ker } \varphi$  donc  $m_i \in \text{Ker } \varphi_i$ . Par suite la projection de  $\mathcal{J}$  sur  $\mathcal{M}_i$  est un idéal de  $\mathcal{M}_i$  contenu dans  $\text{Ker } \varphi_i$  et elle sera donc nulle. D'où  $\mathcal{J} = 0$ .  $\square$

Corollaire. Si  $K$  est un corps, toute algèbre semi-simple de dimension finie est syntactique.

Preuve. En effet, d'après Herstein (1968, th.2.1.7), une telle algèbre est un produit fini d'algèbres simples. Or, une algèbre simple  $\mathcal{M}$  est clairement syntactique, puisqu'elle ne contient que les deux idéaux  $\mathcal{M}$  et  $0$  (le fait que  $K$  est un corps assure l'existence de formes linéaires non nulles).  $\square$

Remarque 2. Une algèbre de Frobenius (Curtis-Renier 10, 61.3) est une algèbre contenant un hyperplan ne contenant ni idéal à gauche, ni idéal à droite non nul. Une telle algèbre est donc clairement syntactique. Comme on le voit, les notions d'algèbre syntactique et d'algèbre de Frobenius sont très voisines. Une autre notion voisine est celle d'algèbre symétrique (ibid. 10, 66). Une telle algèbre est aussi syntactique.

Remarque 3. On peut associer à tout couple  $(\mathcal{M}, \varphi)$  formé d'une algèbre  $\mathcal{M}$  et d'une forme linéaire  $\varphi$  sur  $\mathcal{M}$  une algèbre syntactique (c'est le quotient de  $\mathcal{M}$  par le plus grand idéal contenu dans  $\text{Ker } \varphi$ ). Cela nous amène à la notion de " $\varphi$ -algèbre", analogue à celle des monoïdes pointés de Sakarovitch (1979). Nous ne ferons qu'effleurer ce point.

Remarque 4. Si  $K$ , au lieu d'être un anneau, est un demi-anneau, on peut encore définir l'algèbre syntactique d'une série formelle. La notion d'idéal est remplacée par celle de congruence d'algèbre : la congruence syntactique  $\sim_S$  de la série  $S$  est définie par

$$P \sim_S Q \Leftrightarrow \forall R_1, R_2 \in K\langle X \rangle, (S, R_1 PR_2) = (S, R_1 QR_2)$$

et

$$\mathcal{M}_S = K\langle X \rangle / \sim_S.$$

La propriété universelle du théorème 1 est encore valable mais on ne peut plus formuler le théorème de Kleene-Schützenberger en termes d'algèbre syntactique (voir la remarque 2 du § 1, chap. III).

Remarque 5. On peut définir, en algèbre universelle, une notion d'algèbre syntactique pour toute partie d'un ensemble muni d'une structure algébrique (cf. Steinby, 1979). Les constructions des remarques précédentes apparaissent alors comme des cas particuliers de cette construction très générale, qui inclut celle du monoïde syntactique d'un langage.

## 2. LIENS AVEC LE MODULE SÉRIEL.

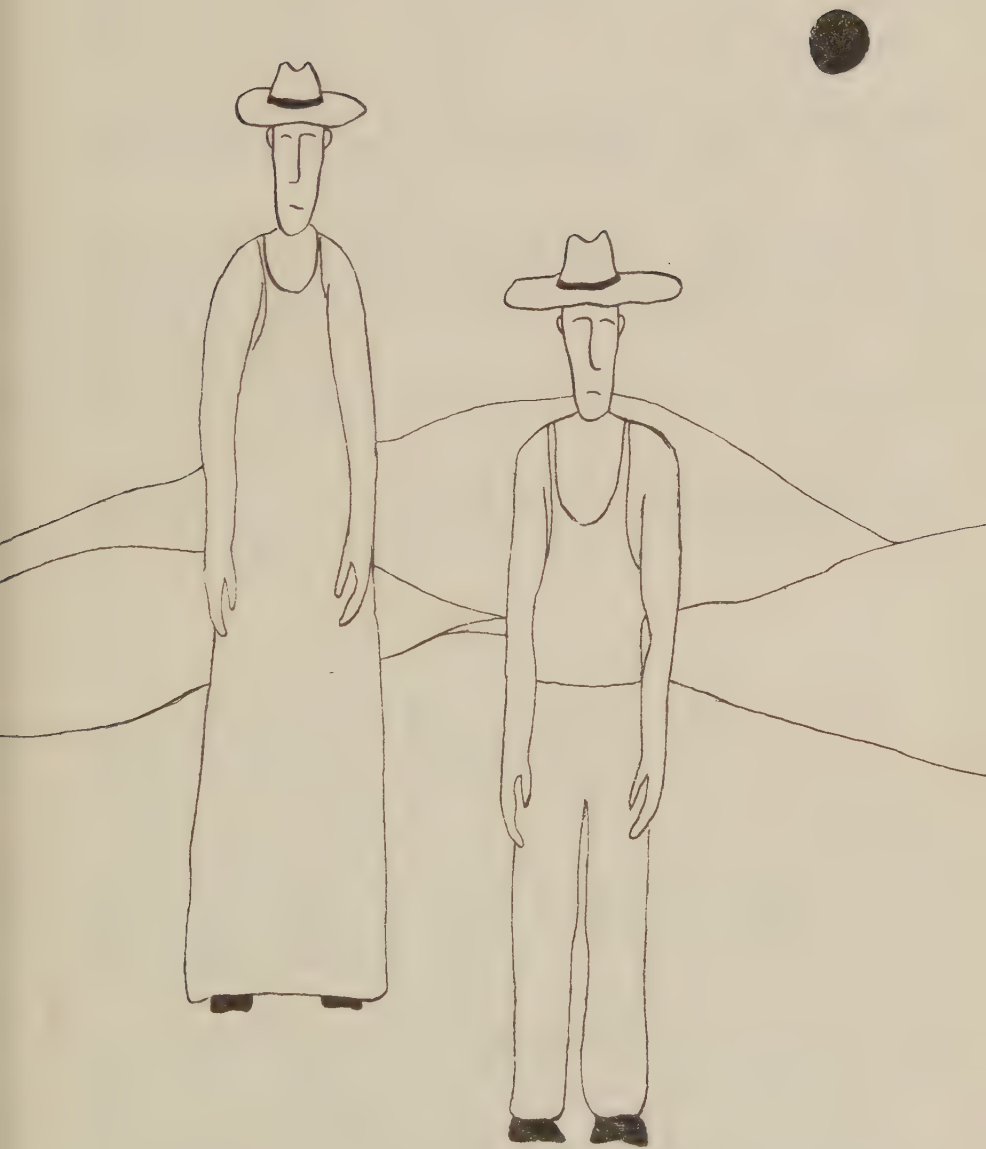
Fliess (1974, p. 207) pose la définition suivante :

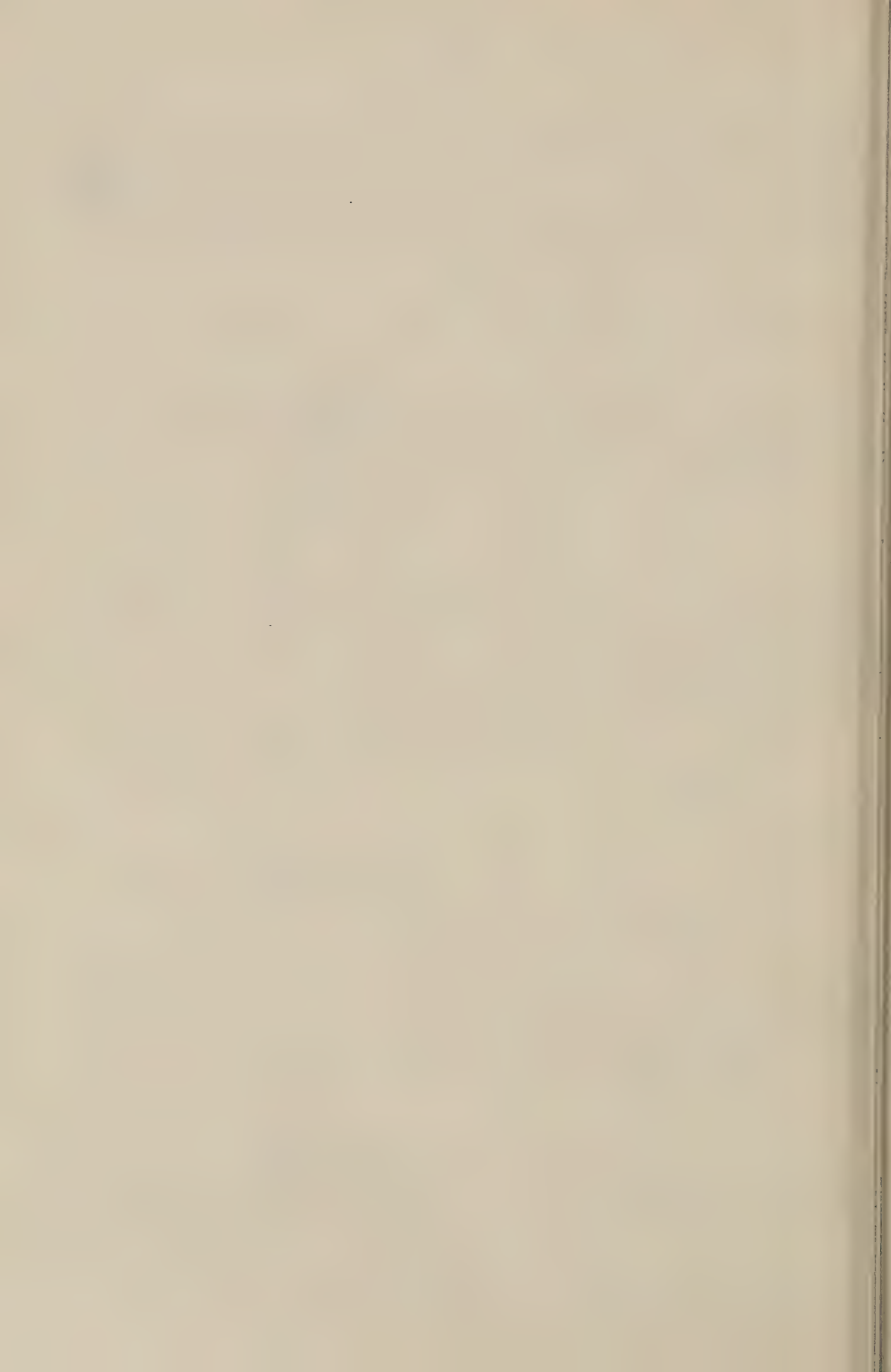
Définition 1. Un  $K\langle X \rangle$ -module sériel gauche est un triplet  $(M, m, \varphi)$  où  $M$  est un  $K\langle X \rangle$ -module à gauche,  $m$  un élément de  $M$  et  $\varphi$  une forme linéaire sur  $M$ . La série reconnue par  $(M, m, \varphi)$  est la série  $S \in K\langle\langle X \rangle\rangle$  définie par

$$(S, w) = \varphi(w m).$$

Le module sériel  $(M, m, \varphi)$  est réduit si  $M$  est engendré par  $m$  comme  $K\langle X \rangle$ -module, et si

$$\{ n \in M \mid \varphi(K\langle X \rangle n) = 0 \} = 0.$$





Nous allons voir qu'il y a des liens étroits entre modules sériels réduits et algèbres syntactiques

Exemple 1. Si  $S \in K\langle\langle X \rangle\rangle$ ,  $S$  est reconnue par le module sériel  $(K\langle X \rangle, 1, S)$  où  $K\langle X \rangle$  est considéré comme  $K\langle X \rangle$ -module à gauche.

Lemme 1. Soit  $M$  un  $K\langle X \rangle$ -module à gauche et  $V$  un sous- $K$ -module de  $M$ . Il existe, parmi les sous- $K\langle X \rangle$ -modules de  $M$  contenus dans  $V$ , un plus grand sous-module.

Preuve. Elle est analogue à celle du lemme 1 du § 1.  $\square$

Définition 1. Soit  $S \in K\langle\langle X \rangle\rangle$ . L'idéal syntactique gauche de  $S$  est le plus grand idéal à gauche de  $K\langle X \rangle$  contenu dans  $\text{Ker } S$ . Il est noté  $\mathfrak{J}_S^g$ .

Lemme 2. On a la relation

$$\mathfrak{J}_S^g = \{ P \in K\langle X \rangle \mid \forall Q \in K\langle X \rangle, (S, QP) = 0 \}$$

Preuve. Elle est analogue à celle du lemme 2 du § 2.  $\square$

Soit  $M_S^g = K\langle X \rangle / \mathfrak{J}_S^g$ ,  $p : K\langle X \rangle \rightarrow M_S^g$  le morphisme canonique de  $K\langle X \rangle$ -modules à gauche,  $m_S^g = p(1)$  et  $\varphi_S^g$  la forme linéaire de  $M_S^g$  induite par  $S$  (puisque  $\mathfrak{J}_S^g \subset \text{Ker } S$ ).

Proposition 1. Le module sériel  $(M_S^g, m_S^g, \varphi_S^g)$  est réduit et reconnaît  $S$ .

Preuve. Comme  $p$  est surjectif, si  $n \in M_S^g$ ,  $n = p(Q)$  pour un  $Q \in K\langle X \rangle$  donc  $n = p(Q.1) = Qp(1) = Qm_S^g$  et  $m_S^g$  engendre le  $K\langle X \rangle$ -module  $M_S^g$ .

Soit  $n \in M_S^g$  tel que  $\varphi_S^g(K\langle X \rangle n) = 0$ . Soit  $Q \in K\langle X \rangle$  tel que  $p(Q) = n$ . Alors pour tout  $R \in K\langle X \rangle$ .

$$(S, RQ) = \varphi_S^g(p(RQ)) = \varphi_S^g(Rp(Q)) = \varphi_S^g(Rn) = 0$$

donc  $Q \in J_S^g$ . Par suite,  $n = p(Q) = 0$ .

Le module sériel ci-dessus est donc réduit. Il reconnaît  $S$  car

$$(S, w) = \varphi_S^g(p(w)) = \varphi_S^g(wp(1)) = \varphi_S^g(wm_S^g). \square$$

Remarque 1. Fliess (ibid.) introduit la notion de morphisme de modules sériels et remarque que deux modules sériels reconnaissant la même série sont isomorphes. On peut le montrer aussi en remarquant que si  $(M, m, \varphi)$  est un module sériel réduit reconnaissant  $S$ , alors l'ensemble

$$\{ P \in K\langle X \rangle \mid Pm = 0 \}$$

n'est autre que l'idéal syntactique gauche de  $S$ .

Soit  $(M, m, \varphi)$  un module sériel reconnaissant la série  $S$ . Pour  $P \in K\langle X \rangle$ , soit  $\mu(P)$  l'endomorphisme du  $K$ -module  $M$  défini par

$$\mu(P)(n) = Pn.$$

Alors  $\mu$  est un homomorphisme de  $K$ -algèbres

$$\mu : K\langle X \rangle \rightarrow \text{End}_K(M)$$

$$\text{En effet} \quad \mu(P + Q) = \mu(P) + \mu(Q)$$

$$\text{et} \quad \mu(PQ) = \mu(P) \circ \mu(Q).$$

Donc  $\mu$  est un homomorphisme surjectif de  $K$ -algèbres  $K\langle X \rangle \rightarrow \mathcal{M}$ , avec  $\mathcal{M} = \mu(K\langle X \rangle)$ .

Soit  $\psi$  la forme linéaire sur  $M$

$$\psi(f) = \varphi \circ f(m).$$

Alors  $(M, \mu, \psi)$  est une représentation surjective de  $S$ . En effet,

$$\forall w \in X^*, (S, w) = \varphi(wm) = \varphi(\mu(w)(m)) = \psi \circ \mu(w).$$

Proposition 2. Si  $(M, m, \varphi)$  est réduit,  $(M, \mu, \psi)$  s'identifie à la représentation minimale de  $S$ .

Preuve. Il suffit de vérifier que  $\text{Ker } \mu$  est égal à  $\mathcal{I}_S$ . Par définition, on a  $\text{Ker } \mu \subset \mathcal{I}_S$ . Réciproquement soit  $P \in \mathcal{I}_S$ . On a  $\forall Q, R \in K\langle X \rangle$   
 $(S, QPR) = 0$ .

Soit  $n \in M$ . Alors  $n = Rm$  pour un  $R \in K\langle X \rangle$ . Par suite,  
 $\forall Q \in K\langle X \rangle$

$$\begin{aligned} \varphi(Q\mu(P)(n)) &= \varphi(QPn) = \varphi(QPRm) = \varphi(\mu(QPR)(m)) \\ &= \psi \circ \mu(QPR) = (S, QPR) = 0 \end{aligned}$$

donc  $\varphi(K\langle X \rangle \mu(P)(n)) = 0$  et  $\mu(P)(n) = 0$

puisque  $(M, m, \varphi)$  est réduit. Par suite,  $\mu(P) = 0$  et  $\mathcal{I}_S \subset \text{Ker } \mu$ .  $\square$

Remarque 2. Tout ce qui a été dit dans ce paragraphe peut être dit en remplaçant "gauche" par "droit". En particulier, on définit l'idéal syntactique droit de  $S$  par

$$\mathcal{I}_S^d = \{ P \in K\langle X \rangle \mid \forall R \in K\langle X \rangle, (S, PR) = 0 \}$$

3. LIENS AVEC LES LANGAGES.

Soit  $L$  un langage sur l'alphabet  $X$ . Son monoïde syntactique est par définition

$$M_L = X^* / \sim_L$$

où  $\sim_L$  est la congruence syntactique de  $L$  définie par :  $w \sim_L w'$  si et seulement si

$$\forall u, v \in X^*, \quad uwv \in L \Leftrightarrow uw'v \in L.$$

(cf. Eilenberg 1974, chap. III, § 10).

Proposition 1. Soit  $S$  la série caractéristique de  $L$ . On a :  $w \sim_L w'$  si et seulement si  $w - w' \in \mathcal{J}_S$ . Par suite, le monoïde syntactique de  $L$  est isomorphe à l'image  $\mu_S(X^*)$  de  $X^*$  dans  $\mathcal{M}_S$ .

Preuve. On a, d'après le lemme 2 du § 1 :  $w - w' \in \mathcal{J}_S$  si et seulement si  $\forall u, v \in X^*, \quad (S, u(w - w')v) = 0$

$$\Leftrightarrow (S, uwv) = (S, uw'v)$$

ce qui est équivalent à

$$uwv \in L \Leftrightarrow uw'v \in L. \quad \square$$

Soit  $K[M_L]$  la  $K$ -algèbre du monoïde  $M_L$ .

Proposition 2.  $\mathcal{M}_S$  est quotient de  $K[M_L]$ .

Preuve. Soit  $\varphi$  l'homomorphisme canonique de monoïdes

$$\varphi : X^* \longrightarrow M_L.$$

$\varphi$  se prolonge en un unique homomorphisme surjectif d'algèbres

$$\mu : K\langle X \rangle \longrightarrow K[M_L]$$

défini par

$$\mu(P) = \sum_{w \in X^*} (P, w) \varphi(w)$$

Soit  $\varphi$  la forme linéaire sur  $K[M_L]$  définie par sa valeur sur la base  $M_L$  de  $K[M_L]$

$$\begin{aligned} \varphi(m) &= 1 & \text{si } m \in \varphi(L) \\ \varphi(m) &= 0 & \text{si } m \notin \varphi(L). \end{aligned}$$

Alors  $\forall w \in X^*$

$$\begin{aligned} \varphi \circ \mu(w) = \varphi \circ \varphi(w) &= 1 & \text{si } \varphi(w) \in \varphi(L) & \text{i.e. } w \in L \\ & & \text{i.e. } (S, w) = 1 \\ &= 0 & \text{si } \varphi(w) \notin \varphi(L) & \text{i.e. } w \notin L \\ & & \text{i.e. } (S, w) = 0 \end{aligned}$$

Par suite  $S = \varphi \circ \mu$ .

Donc  $(K[M_L], \mu, \varphi)$  est une représentation surjective de  $S$ . D'après le théorème 1 du § 1,  $\mathcal{M}_S$  est quotient de  $K[M_L]$ .  $\square$

Remarque 1. Hotz (1976) appelle algèbre syntactique de  $L$  l'algèbre  $K[M_L]$ . Nous venons de voir que l'algèbre syntactique de la série caractéristique de  $L$ , telle que nous la définissons, est quotient de  $K[M_L]$ . On n'a pas isomorphisme en général comme le montre l'exemple suivant :

$$X = \{x\}, \quad L = (1+x)(x^4)^*$$

On vérifie aisément que  $\sim_L$  est engendrée par l'unique relation

$$x^4 \sim_L 1$$

Par suite,  $M_L \simeq \mathbb{Z}/4\mathbb{Z}$  a 4 éléments, et  $K[M_L]$  est de dimension 4 (nous supposons que  $K$  est un corps).

Cependant, si  $S$  est la série caractéristique de  $L$ , on vérifie sans peine que

$$1 - x + x^2 - x^3 \in J_S.$$

Par suite  $\mathcal{H}_S$  est de dimension au plus 3.

Eilenberg (1976) appelle *rigide* un langage dont la congruence syntactique est l'égalité.

Définition 1. Une série formelle est *rigide* si son idéal syntactique est nul.

Nous allons voir qu'il existe des séries formelles rigides ; rappelons à ce sujet que le langage des mots *palindromes*, i.e. les mots qui sont égaux à leur image miroir ( $w$  de  $w$  se définit comme suit :  $\tilde{1} = 1$  et si  $w = uv$ ,  $\tilde{w} = \tilde{v}\tilde{u}$ ) est rigide lorsque  $\text{Card}(X) \geq 2$ . Nous montrons plus loin que la série caractéristique des mots palindromes est rigide. Auparavant nous prouvons un lemme technique de théorie des langages.

Lemme 1. Soit  $L = \{w \in X^* \mid w = \tilde{w}\}$  et  $\text{Card}(X) \geq 2$ . Soient  $u, v_1, \dots, v_n \in X^*$  tels que  $u \neq v_1, \dots, v_n$  et  $|u| \leq |v_1|, \dots, |v_n|$ . Il existe  $w \in X^*$  tel que  $uw \in L$  et  $v_1w, \dots, v_nw \notin L$ .

Preuve. Soit  $p = \sup \{|v_i| - |u|, i = 1, \dots, n\}$  et  $w = x^p y y x^p$ ,  $x \neq y$ ,  $x, y \in X$ . On a  $uw = u x^p y y x^p \tilde{u} \in L$ .

Soit  $i \in \{1, \dots, n\}$  et supposons  $v_i w \in L$ . Alors  $\widetilde{v_i w} = v_i w$  i.e.  $\tilde{v_i} \tilde{w} = v_i w$  donc  $v_i w = u x^p y y x^p \tilde{v_i}$ . Il existe donc, puisque  $|u| \leq |v_i|$  un mot  $t$  tel que  $v_i = ut$ . Donc  $v_i w = ut x^p y y x^p \tilde{u} \tilde{t}$   $\in L$  et par suite  $t x^p y y x^p \in L$ . Or  $|t| \leq p$  implique  $t = x^{p+q} y y x^p$   $\in L$ , ce qui est absurde.  $\square$

Proposition 3. Si  $\text{Card}(X) \geq 2$ , la série caractéristique des mots palindromes est rigide.

Preuve. Soit  $L$  le langage des mots palindromes et  $S$  sa série caractéristique. Supposons  $\mathcal{J}_S \neq 0$  et soit  $P \in \mathcal{J}_S$ ,  $P \neq 0$ .

P s'écrit  $P = \lambda_u + \lambda_1 v + \dots + \lambda_n v_n$  avec  $\lambda \in K \setminus 0$ ,  $|\lambda| \leq |v_1|, \dots, |v_n|$ . D'après le lemme, il existe  $w \in X^*$  tel que  $uw \in L$ ,  $v_1 w, \dots, v_n w \notin L$ . Alors  $Pw \in \mathcal{J}_S \Rightarrow 0 = (S, Pw) = \lambda$  ce qui est absurde.  $\square$

Remarque 2. Nous avons montré en fait que l'idéal syntactique droit de  $S$  est nul. Donc  $\text{Ker } S$  ne contient aucun idéal à droite non nul (et de même pour les idéaux à gauche).

Corollaire.  $K\langle X \rangle$  est une algèbre syntactique.

Preuve. Nous venons de le voir quand  $\text{Card}(X) \geq 2$ . Si  $X = \{x\}$ , on vérifie que la série caractéristique de  $\{x^{n^2} \mid n \in \mathbb{N}\}$  est rigide.

#### 4. CHANGEMENT D'ANNEAU.

Soit  $L$  un sur-anneau commutatif de  $K$ . On a les injections canoniques

$$K\langle X \rangle \longrightarrow L\langle X \rangle$$

$$K\langle\langle X \rangle\rangle \longrightarrow L\langle\langle X \rangle\rangle$$

Par ailleurs on a l'identification suivante

$$L\langle X \rangle \simeq K\langle X \rangle \otimes_K L.$$

Proposition 1. Soit  $S \in K\langle\langle X \rangle\rangle$  et  $R = (\mathbb{M}, \mu, \varphi)$  une  $K$ -représentation de  $S$ . Alors  $S$ , considérée comme élément de  $L\langle\langle X \rangle\rangle$  admet la  $L$ -représentation

$$R' = (\mathbb{M} \otimes_K L, \mu \otimes_K \text{id}, \varphi \otimes_K \text{id})$$

où  $\text{id}$  désigne l'identité  $L \rightarrow L$ . Si  $R$  est surjective (resp. finie)  $L$ 'est aussi.

Preuve. Si  $w \in X^*$

$$(\varphi \otimes \text{id}) \circ (\mu \otimes \text{id})(w) = (\varphi \otimes \text{id})(\mu(w) \otimes 1) = \varphi \circ \mu(w) = (S, w)$$

Proposition 2. (Hypothèses de la proposition 1). On suppose de plus que  $L$  est un corps et que  $R$  est la  $K$ -représentation minimale de  $S$ . Alors  $S$  s'identifie à la  $L$ -représentation minimale de  $S$ .

Preuve.  $S$ , considérée comme élément de  $L\langle\langle X \rangle\rangle$ , a pour idéal syntactique

$$\mathcal{I}_S^L = \{P \in L\langle X \rangle \mid \forall u, v \in X^*, (S, uPv) = 0\}.$$

Il suffit de montrer que  $\mathcal{I}_S^L = \text{Ker}(\mu \otimes \text{id})$ . Or,  $\text{Ker}(\mu \otimes \text{id}) \subset \text{Ker}(\mu)$  donc  $\text{Ker}(\mu \otimes \text{id}) \subset \mathcal{I}_S^L$ .

Soit  $P \in \mathcal{I}_S^L$  et  $(\ell_i)_{i \in I}$  une base de  $L$  considéré comme  $K$ -espace vectoriel. Alors on a l'isomorphisme d'espaces vectoriels sur  $K$

$$L\langle X \rangle = K\langle X \rangle \otimes L \cong \bigoplus_{i \in I} K\langle X \rangle \otimes \ell_i$$

Donc  $P = \sum P_i \otimes \ell_i$  avec des  $P_i \in K\langle X \rangle$  presque tous nuls.

Soient  $u, v \in X^*$ . On a

$$uPv = \sum uP_i v \otimes \ell_i$$

Comme  $P \in \mathcal{J}_S^L$

$$\begin{aligned} 0 &= (S, uPv) = (\psi \otimes \text{id}) \circ (\mu \otimes \text{id}) (uPv) \\ &= (\psi \otimes \text{id}) (\sum \mu(uP_i v) \otimes \ell_i) \\ &= \sum \ell_i \psi \circ \mu(uP_i v) = \sum \ell_i (S, uP_i v). \end{aligned}$$

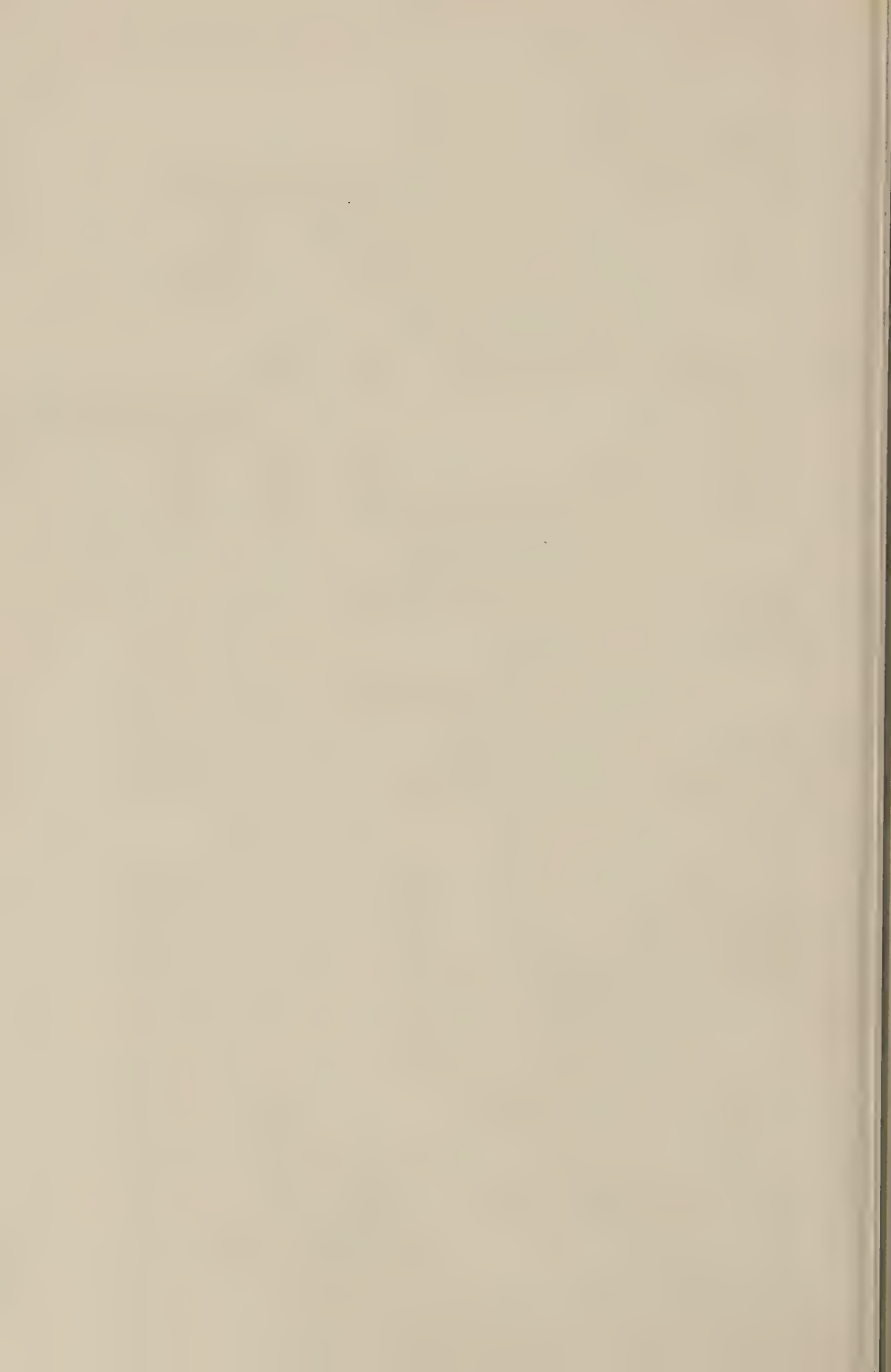
Or :

$$L = \bigoplus K \ell_i$$

Donc pour tout  $i$ ,  $(S, uP_i v) = 0$  et ceci pour tous  $u, v \in X^*$ . Par suite, chaque  $P_i \in K\langle X \rangle$  est dans l'idéal syntactique de  $S$  sur  $K\langle X \rangle$  donc, puisque  $\mathcal{R}$  est minimale, dans  $\text{Ker } \mu$ . D'où

$$(\mu \otimes \text{id})(P) = \sum \mu(P_i) \otimes \ell_i = 0 \quad \text{et}$$

$$P \in \text{Ker } (\mu \otimes \text{id}). \quad \square$$



### CHAPITRE III

## ALGÈBRES SYNTACTIQUES DES SÉRIES RATIONNELLES

-----

Ici commencent les choses sérieuses. Le théorème de Kleene-Schützenberger s'exprime en termes d'algèbres syntactiques : une série est rationnelle si et seulement si son algèbre syntactique est de dimension finie (th. 1, § 1). Ceci permet de ramener le problème de la rationalité des séries et aussi des langages à des problèmes classiques d'algèbre, les problèmes de Kurosch et de Burnside. Nous utilisons un théorème de Chirchov (§ 2) sur les algèbres vérifiant une identité polynômiale pour établir au § 3 un critère de rationalité des séries (th. 1, § 3). Ce critère ramène la rationalité d'une série, lorsque son algèbre syntactique vérifie une identité polynômiale, à un nombre fini de rationalités locales ; plus précisément, sous les hypothèses sus-mentionnées, une série est rationnelle si et seulement si un nombre (essentiellement) fini de séries en une variable, qui lui sont canoniquement associées, sont rationnelles et vérifient une relation de récurrence linéaire commune. Ces séries d'une variable s'obtiennent par restriction aux *rayons*, ce qui est un procédé habituel en théorie des langages.

Les implications de notre théorème sont nombreuses. Il permet notamment un transfert de certaines propriétés arithmétiques des séries rationnelles en une variable aux séries en plusieurs variables, ce que nous illustrons aux chapitres 4, 6 et 7. Une autre application est un critère de rationalité des langages (th. 2, § 3) dont on déduit un résultat (prop. 2, § 3) sur les langages rationnels qui est en un certain sens orthogonal au lemme de l'étoile ("pumping lemma").

Au paragraphe 4, nous montrons que tout idéal bilatère de l'algèbre libre admet un système de générateurs d'une forme très particulière, faisant intervenir les codes facteurs (un code est dit facteur si aucun mot du code n'est facteur d'un autre mot du code). Cette méthode est assez générale, et s'applique aussi bien aux idéaux à droite de l'algèbre libre (les codes qui interviennent dans ce cas sont des codes préfixes, et l'on peut redémontrer un théorème de Cohn sur la liberté de ces idéaux) qu'aux idéaux de l'algèbre des polynômes commutatifs (ce qui permet de retrouver, moyennant un théorème de Dickson sur l'ordre dans  $\mathbb{N}^k$ , que cet anneau est noëthérien) ; elle s'applique aussi aux sous-groupes du groupe libre, et aux congruences du monoïde libre et du monoïde commutatif libre. Par restriction aux idéaux syntactiques, nous trouvons des relations de récurrence bilatères pour les séries rationnelles.

Au dernier paragraphe, nous établissons quelques propriétés des séries rationnelles et centrales (i.e. des séries telles que le coefficient d'un mot ne dépende que de sa classe de conjugaison) et leurs liens avec les caractères.

Les conventions adoptées au début du chapitre II sont maintenues ici, excepté que les alphabets seront toujours supposés *finis*. Nous ferons souvent usage de l'abus suivant : si  $\nu$  est un homomorphisme de monoïdes

$$X^* \longrightarrow K^{n \times n}$$

nous appellerons encore  $\nu$  son extension

$$K \langle X \rangle \longrightarrow K^{n \times n}$$

(sans le rappeler explicitement dans le texte). Rappelons encore que nous confondons toute série formelle avec la forme linéaire qu'elle définit sur  $K\langle X \rangle$ .

## 1 - LE THEOREME FONDAMENTAL

Le théorème de Kleene-Schützenberger (th. 1 § 3, chap. I) admet une formulation en termes d'algèbres syntactiques.

Théorème 1 - Soit  $S \in K\langle\langle X \rangle\rangle$ . Les conditions suivantes sont équivalentes :

- (i)  $S$  est rationnelle
- (ii)  $S$  admet une représentation finie
- (iii)  $M_S$  est un module de type fini

(Avec les conventions suivantes,  $K$  étant fixé une fois pour toutes : rationnel signifie  $K$ -rationnelle, représentation =  $K$ -représentation, module =  $K$ -module)

Preuve (i)  $\Rightarrow$  (iii)  $S$  est reconnaissable (th. 1, § 3, chap. I) et admet la représentation linéaire  $(\lambda, \nu, \gamma)$  où

$$\nu : X^* \rightarrow K^{n \times n}$$

est un homomorphisme. Soit  $K_1$  le sous-anneau de  $K$  engendré par l'ensemble fini des coefficients des matrices  $\lambda, \gamma$  et  $\nu x$ ,  $x \in X$ .  $K_1$  est un anneau de type fini (i.e. une  $\mathbb{Z}$ -algèbre de type fini) donc d'après un théorème de Hilbert, c'est un anneau noethérien. Soit

$$M = \nu(K_1\langle X \rangle)$$

et  $\varphi$  la forme  $K_1$ -linéaire sur  $M$

$$\varphi(m) = \lambda m \gamma$$

Alors  $(M, \nu, \varphi)$  est une  $K_1$ -représentation surjective de  $S$  ; elle est de plus finie, car  $M$  est un sous-module du modèle noethérien  $K_1^{n \times n}$ .

Par suite  $(M \otimes_{K_1} K, \nu \otimes_{K_1} \text{id}, \varphi \otimes_{K_1} \text{id})$  est une  $K$ -représentation finie et surjective de  $S$  (prop. 1, § 4, chap. I). D'après le th. 1 du § 1, chap. II,  $M_S$  est quotient de  $M \otimes K$ , donc c'est un  $K$ -module de type fini.

(iii)  $\Rightarrow$  (ii) C'est clair.

(ii)  $\Rightarrow$  (i) Soit  $(M, \mu, \varphi)$  une représentation finie de  $S$  et  $m_1, \dots, m_n$  des générateurs du  $K$ -module  $M$ . Il existe des matrices

$$M_x = (a_{ij}^x)_{1 \leq i, j \leq n} \in K^{n \times n}$$

telles que  $\forall x \in X, \forall j \in \{1, \dots, n\}$

$$\mu x. m_j = \sum_i a_{ij}^x m_i$$

Soit  $\nu$  l'homomorphisme  $X^* \rightarrow K^{n \times n}$  tel que  $\nu x = M_x$ . On vérifie alors, par récurrence sur la longueur du mot  $w$  que

$$\mu w. m_j = \sum_i (\nu w)_{i,j} m_i$$

Soient  $\lambda \in K^{1 \times n}$ ,  $\gamma \in K^{n \times 1}$  définis par

$$\varphi(m_i) = \lambda_i \quad \text{et} \quad 1 = \sum_j \gamma_j m_j$$

Alors

$$\mu w = \mu w. 1 = \sum_j \mu w. m_j \cdot \gamma_j = \sum_{i,j} (\nu w)_{i,j} \cdot m_i \cdot \gamma_j$$

donc

$$(S, w) = \varphi \circ \mu w = \sum_{i,j} \lambda_i \cdot (\nu w)_{i,j} \cdot \gamma_j = \lambda \cdot \nu w \cdot \gamma$$

Par suite  $S$  est reconnaissable, donc rationnelle.  $\square$

Remarque 1 - L'implication (i)  $\Rightarrow$  (iii) est immédiate lorsque  $K$  est un corps (ou un anneau noethérien). Dans le cas général, nous avons utilisé un argument de Sontag (1975) qui a étendu aux anneaux une propriété de Hankel des séries rationnelles déjà établie pour les corps par Fliess (1974).

Remarque 2 (ici le lecteur est prié de relire la remarque 4 du § 1, chap. II)

Le théorème 1 n'est plus valable si  $K$  est un demi-anneau. En effet soit  $K = \mathbb{R}_+$  et  $S = \sum_{n \geq 0} n x^n$ .  $S$  est  $\mathbb{R}_+$ -rationnelle car elle admet la représentation linéaire  $(\lambda, \nu, \gamma)$  avec

$$\lambda = (1, 0) \quad \nu x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \gamma = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Soit  $\mathcal{M} = \nu(\mathbb{R}_+[x])$ . Alors  $\mathcal{M}$  est l'algèbre syntactique de  $S$  considérée comme élément de  $\mathbb{R}_+[[x]]$ . En effet, soient  $P, Q \in \mathbb{R}_+[x]$

$$P = a_0 + a_1 x + \dots + a_k x^k, \quad Q = b_0 + b_1 x + \dots + b_k x^k$$

Alors

$$P \sim_S Q$$

$$\text{ssi} \quad \forall n \in \mathbb{N}, (S, Px^n) = (S, Qx^n)$$

$$\text{ssi} \quad \forall n, \sum (n+i) a_i = \sum (n+i) b_i$$

$$\text{ssi} \quad \sum a_i = \sum b_i \quad \text{et} \quad \sum i a_i = \sum i b_i$$

$$\text{ssi} \quad \nu P = \begin{pmatrix} \sum a_i & \sum i a_i \\ 0 & \sum a_i \end{pmatrix} = \begin{pmatrix} \sum b_i & \sum i b_i \\ 0 & \sum b_i \end{pmatrix} = \nu Q.$$

Supposons que  $\mathcal{M}$  soit un  $\mathbb{R}_+$ -module de type fini. Comme les matrices  $\nu x^n$ ,  $n \in \mathbb{N}$ , engendrent  $\mathcal{M}$ , il existe un  $p$  tel que  $\nu x^p$  soit une combinaison linéaire des  $\nu x^i$ ,  $i < p$ .

$$\nu x^p = \sum_{i < p} \lambda_i \nu x^i$$

Par suite,  $\forall n \in \mathbb{N}$

$$\nu x^{p+n} = \sum \lambda_i \nu x^{i+n}$$

Donc

$$p+n = \sum_i \lambda_i (i+n) \quad \forall n \in \mathbb{N}$$

et ceci implique  $1 = \sum \lambda_i$  et  $p = \sum i \lambda_i = \sum_{i < p} i \lambda_i < p$

$$\sum (p-1) \lambda_i = p-1$$

ce qui est absurde.

Remarque 3 On suppose que  $K$  est un corps. Soit  $S = \sum a_n x^n$  une série d'une variable. On sait qu'elle est rationnelle si et seulement si elle vérifie une relation de récurrence linéaire, i.e. s'il existe des coefficients

$$\alpha_1, \dots, \alpha_k \in K \text{ tels que}$$

$$\forall n \in \mathbb{N}, \quad a_{n+k} = \alpha_1 a_{n+k-1} + \dots + \alpha_k a_n.$$

La longueur de la relation de récurrence est l'entier  $k$  ; le polynôme associé à la relation est

$$P = x^k - \alpha_1 x^{k-1} - \dots - \alpha_k.$$

Il n'est pas difficile de voir que l'algèbre syntactique de  $S$  est isomorphe à

$$K[x] / (P)$$

si la relation ci-dessus est choisie de longueur minimum.

L'hypothèse que  $K$  est un corps peut être affaiblie : il suffit de supposer que  $K$  est un anneau intégralement clos dans son corps des fractions  $F$  (en effet, dans ce cas, le polynôme minimal sur  $F$  d'un élément entier algébrique sur  $K$  est à coefficients dans  $K$ ). Cependant, dans le cas général, les considérations ci-dessus ne sont plus vraies : en effet, soit  $K = \mathbb{Z}[\sqrt{5}]$

$$\alpha = \frac{\sqrt{5} + 1}{2}, \quad S = \sum 2 \alpha^n x^n.$$

Alors  $S$  est  $K$ -rationnelle puisque

$$\alpha^2 = \alpha + 1.$$

La plus courte relation que vérifie  $S$  est associée au polynôme

$$x^2 - x - 1$$

mais  $K[X] / (x^2 - x - 1)$  n'est pas l'algèbre syntactique de  $S$  puisque l'on a

$$2x \equiv \sqrt{5} + 1 \pmod{\mathcal{J}_S}$$

comme on le vérifie aisément.

Nous allons préciser maintenant le lien entre représentation minimale d'une série rationnelle et représentation linéaire réduite. Il s'ensuivra en particulier que l'on peut "calculer" dans l'algèbre syntactique d'une série rationnelle donnée, puisque l'on sait en déterminer une représentation linéaire réduite (Schützenberger 1961).

Théorème 2. On suppose que  $K$  est un corps. Soit  $(\lambda, \nu, \gamma)$  une représentation linéaire réduite de la série rationnelle  $S$ . Soit  $\mathcal{M} = \nu(K\langle X \rangle)$  et la forme linéaire sur  $K$  définie par

$$\psi(m) = \lambda m \gamma.$$

Alors  $(\mathcal{M}, \nu, \psi)$  s'identifie à la représentation minimale de  $S$ .

Preuve. D'après Fliess (1974), les espaces vectoriels  $\lambda \mathcal{M}$  et  $\mathcal{M} \gamma$  sont de dimension exactement  $n = \dim(\nu)$ , sinon  $S$  admettrait une représentation linéaire de dimension  $< n$  et  $(\lambda, \nu, \gamma)$  ne serait pas réduite. Par

$$\lambda \mathcal{M} = K^{1 \times n}, \quad \mathcal{M} \gamma = K^{n \times 1}$$

Soit  $P \in \mathcal{J}_S$  : alors  $\forall Q, R \in K\langle X \rangle$ ,  $0 = (S, QPR) = (\lambda, \nu P(\nu R, \gamma))$  donc  $K^{1 \times n} \cdot \nu P \cdot K^{n \times 1} = 0 \Rightarrow \nu P = 0$ . D'où  $\mathcal{J}_S \subset \text{Ker } \nu$ .

L'inclusion inverse résulte de la définition de  $\mathcal{J}_S$ . On a donc  $\mathcal{J}_S = \text{Ker } \nu$ . Soit  $S = \psi \circ \nu$ , donc  $(\mathcal{M}, \nu, \psi)$  s'identifie à la représentation minimale de  $S$ .

□

Dans le cas où  $K$  est un corps, on peut préciser la dimension de l'algèbre syntactique d'une série rationnelle à l'aide de l'opérateur  $\circ$  introduit au chapitre I, § 3. Rappelons que si  $S \in K\langle\langle X \rangle\rangle$ ,  $u, v \in X^*$  la série  $u \circ S \circ v$  est définie par

$$(u \circ S \circ v, w) = (S, vw u)$$

Proposition 1. On suppose que  $K$  est un corps. Soit  $E$  le sous-espace de  $K\langle\langle X \rangle\rangle$  engendré par les séries  $u \circ S \circ v$  ( $u, v \in X^*$ ), où  $S$  est une série rationnelle. Alors l'orthogonal de  $E$  dans  $K\langle\langle X \rangle\rangle$  est égal à  $\mathcal{I}_S$  et l'orthogonal de  $\mathcal{I}_S$  dans  $K\langle X \rangle$  est égal à  $E$ . En particulier le dual de  $\mathcal{M}_S$  est isomorphe à  $E$ , par l'application qui à une forme linéaire  $\varphi$  sur  $\mathcal{M}_S$  associe la série  $\varphi \circ \mu_S$ . On a donc

$$\dim \mathcal{M}'_S = \dim \mathcal{I}_S^o$$

Preuve. Soit  $E^o$  l'orthogonal de  $E$ . On a :

$$\begin{aligned} P \in E^o &\Leftrightarrow \forall u, v \in X^* & (u \circ S \circ v, P) &= 0 \\ &\Leftrightarrow \forall u, v \in X^* & (S, v P u) &= 0 \\ &\Leftrightarrow P \in \mathcal{I}_S & (\text{lemme 2 du § 1, chap. II}) \end{aligned}$$

Soit  $\mathcal{M}'_S$  le dual de  $\mathcal{M}_S$  et  $\alpha$  l'application linéaire

$$\begin{aligned} \mathcal{M}'_S &\rightarrow K\langle\langle X \rangle\rangle \\ \varphi &\mapsto \varphi \circ \mu_S \end{aligned}$$

On a  $\text{Ker}(\varphi \circ \mu_S) \subset \text{Ker} \mu_S = \mathcal{I}_S$ , donc l'image de  $\alpha$  est contenue dans  $\mathcal{I}_S^o$  (l'orthogonal de  $\mathcal{I}_S$  dans  $K\langle\langle X \rangle\rangle$ ). De plus, si  $T \in \mathcal{I}_S^o$ , on a  $\text{Ker} \mu_S \subset \text{Ker} T$ , donc  $T$  définit sur  $\mathcal{M}_S$  une forme linéaire  $\varphi$  vérifiant  $\varphi \circ \mu_S = T$ . Par suite  $\alpha(\mathcal{M}'_S) = \mathcal{I}_S^o$ . Par ailleurs,  $\alpha$  est clairement injective puisque  $\mu_S$  est surjective. Par suite  $\mathcal{M}'_S$  est isomorphe à  $\mathcal{I}_S^o$ .

Jusqu'à présent nous n'avons pas utilisé l'hypothèse que  $S$  est rationnelle. Elle va nous servir à présent. Comme

$$E \subset E^{00} = \mathcal{U}_S^0$$

on a  $\dim(E) \leq \dim(\mathcal{M}_S') = \dim(\mathcal{M}_S) < \infty$

donc on a l'égalité

$$E = E^{00} = \mathcal{U}_S^0$$

(Bourbaki 1962, chap. 2, th. 7 du § 7).  $\square$

## 2. UN THEOREME DE CHIRCHOV.

Soit  $S$  une série rationnelle et  $u, v, w$  des mots. Alors la série d'une variable

$$\sum_{n \geq 0} (S, u w^n v) t^n$$

est rationnelle. En effet, si  $(\lambda, \gamma, \delta)$  est une représentation linéaire de  $S$ , la suite  $(S, u w^n v)$  vérifie une relation de récurrence linéaire déterminée par le polynôme caractéristique de la matrice  $\gamma w$ .

Cette propriété ne caractérise pas les séries rationnelles comme le montre l'exemple de la série caractéristique du langage

$$L = \{ w, \quad |w|_x = |w|_y \}$$

sur l'alphabet  $\{x, y\}$ . Cette série n'est pas rationnelle sinon  $L$  serait un langage rationnel (cor. 4 à la prop. 3, § 3, chap. I).

Nous allons donner, au paragraphe suivant, une condition supplémentaire qui, jointe à la propriété ci-dessus, caractérise la rationalité des séries. Ce problème est intimement lié au problème de Kurosch : Si  $\mathcal{M}$  est une algèbre de type fini et de torsion (i.e. tout  $x \in \mathcal{M}$  engendre une sous-algèbre qui est un  $K$ -module de type fini, ce qu'on exprime aussi en disant que  $x$  est entier algébrique

sur  $K$  i.e. annule un polynôme sur  $K$  de coefficient dominant 1) si  $\mathcal{H}$ , disais-je, est une telle algèbre, peut-on en déduire que  $\mathcal{H}$  est un  $K$ -module de type fini ? Par ailleurs, si l'on s'intéresse non plus aux séries mais aux langages, le problème analogue est le problème de Burnside : Si  $M$  est un monoïde de type fini et de torsion (i.e. tout  $x \in M$  engendre un sous-monoïde fini) est-ce que  $M$  est fini ?

Les problèmes de Burnside et de Kurosch, formulés ainsi dans toute leur généralité, ont reçu tous deux une réponse négative (voir Herstein 1968, chap. VIII). Cependant, lorsqu'on se restreint aux algèbres à *identité polynômiale*, le problème de Kurosch se voit répondre par l'affirmative.

Rappelons qu'une  $K$ -algèbre  $\mathcal{H}$  vérifie une *identité polynômiale* s'il existe un alphabet  $X = \{x_1, \dots, x_k\}$  et un polynôme  $P(x_1, \dots, x_k) \in K\langle X \rangle$  non nul tel que

$$\forall m_1, \dots, m_k \in \mathcal{H} \quad P(m_1, \dots, m_k) = 0$$

Le *degré* de l'identité est le degré de  $P$ . L'identité est dite *admissible* (selon Chirchov) s'il y a dans le support de  $P$  un mot  $w$  de longueur maximum i.e.  $|w| = \deg(P)$  qui vérifie  $(P, w) = 1$ . (On remarquera que si  $K$  est un corps, la condition pour  $P$  d'être admissible est redondante). On montre que si  $\mathcal{H}$  vérifie une identité polynômiale admissible  $\mathcal{M}$  vérifie aussi une *identité multilinéaire* de même degré, de la forme

$$\forall m_1, \dots, m_p \in \mathcal{M}, m_1, \dots, m_p = \sum_{\substack{\sigma \in \mathfrak{S}_p \\ \sigma \neq \text{id}}} \alpha_\sigma m_{\sigma(1)} \dots m_{\sigma(p)}$$

où les  $\alpha_\sigma$  sont dans  $K$ . (Amitsur donne une condition plus faible que l'admissibilité pour qu'il en soit ainsi, voir Procesi, chap. II, th. 4.1.)

Nous utiliserons le théorème suivant, dû à Chirchov (1957, th. 4 ; voir aussi Prosesi 1973 addendum au chap. VI).

Théorème (Chirchov). Soit  $M$  une algèbre vérifiant une identité polynômiale admissible de degré  $n$ . On suppose que  $M$  admet, en tant qu'algèbre, un système générateur fini et que tout élément de  $M$  qui est produit d'au plus  $n$  de ces générateurs est entier algébrique sur  $K$ . Alors  $M$  est un  $K$ -module de type fini.

Remarque 1. Le théorème ci-dessus admet comme conséquence le résultat classique qui dit qu'une algèbre commutative de type fini admettant un système de générateurs algébriques est de dimension finie. Il suffit en effet de voir qu'une telle algèbre vérifie l'identité polynômiale de degré 2

$$xy - yx = 0$$

### 3. UN CRITERE DE RATIONALITE

Nous allons traduire le théorème de Chirchov en termes de séries formelles et obtiendrons un critère de rationalité.

Définition 1. Un *rayon* est une partie de  $X^*$  de la forme  $uw^*v$  ( $u, v, w \in X^*$ ). La *période* du rayon est le mot  $w$ . Si  $R$  est un rayon et  $S$  une série formelle, nous notons  $S(R)$  la série d'une variable

$$S(R) = \sum_{n \geq 0} (S, uw^n v) t^n$$

Théorème 1. Une série formelle  $S$  est rationnelle si et seulement s'il existe un entier  $n$  tel que les deux conditions suivantes soient réalisées.

- (i)  $M_S$  vérifie une identité polynômiale <sup>admissible</sup> de degré  $n$ .

(ii) Pour tout mot  $w$  de longueur  $\leq n-1$  les séries  $S(R)$ , quand  $R$  parcourt l'ensemble des rayons de période  $w$ , vérifient une relation de récurrence linéaire commune.

Preuve. Si  $S$  est rationnelle,  $\mathcal{M}_S$  est un  $K$ -module de type fini (th.1, § 1) et vérifie donc une identité polynômiale (Procesi 1973, th. 3.20, chap. I). De plus,  $S$  est reconnaissable ; soit  $(\lambda, \nu, \gamma)$  une représentation linéaire de  $S$ . Alors la série

$$\sum_{p \geq 0} (S, uw^p v) t^p$$

vérifie la relation de récurrence linéaire définie par le polynôme caractéristique de  $\gamma w$ , qui ne dépend que de la période  $w$  du rayon  $uw^*v$ .

Réciproquement, soit  $S$  une série formelle vérifiant (i) et (ii) et  $w$  un mot de longueur  $\leq n-1$ . Il existe par hypothèse un entier  $k \geq 1$  et des  $a_i \in K$  tels que pour tous mots  $u, v$  et tout entier  $p \geq 0$

$$(S, uw^{p+k} v) = \sum_{0 \leq i \leq k-1} a_i (S, uw^{p+i} v)$$

En particulier, pour tous mots  $u, v$

$$(S, uw^k v) = \sum a_i (S, uw^i v)$$

$$\text{i.e.} \quad (S, u(w^k - \sum a_i w^i) v) = 0$$

et par suite (lemme 2, § 1, chap. II)

$$w^k - a_{k-1} w^{k-1} - \dots - a_0 \in \mathcal{J}_S$$

et  $\mu_S(w)$  est entier algébrique sur  $K$ . Comme  $\mu_S(X)$  est un système générateur de la  $K$ -algèbre  $\mathcal{M}_S$ , le théorème de Chirchov assure que  $\mathcal{M}_S$  est un  $K$ -module de type fini.  $\square$

Nous pouvons aussi tirer du théorème de Chirchov un critère de rationalité pour les langages. Un des arguments utilisés est le fait qu'un langage est rationnel si et seulement si sa série caractéristique est rationnelle (ceci est le corollaire 4 au théorème 1, § 3, chapitre I).

On notera l'analogie entre le résultat qui suit et le fameux problème de Thierrin : est-ce qu'un langage algébrique dont le monoïde syntactique est de torsion est rationnel ?

Théorème 2. Soit  $L$  un langage et  $S$  sa série caractéristique. Alors  $L$  est rationnel si et seulement si l'algèbre syntactique de  $S$  vérifie une identité polynômiale et si le monoïde syntactique de  $L$  est de torsion.

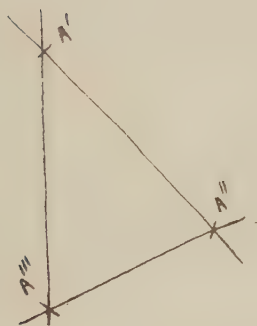
Preuve. Que la condition soit nécessaire est clair.

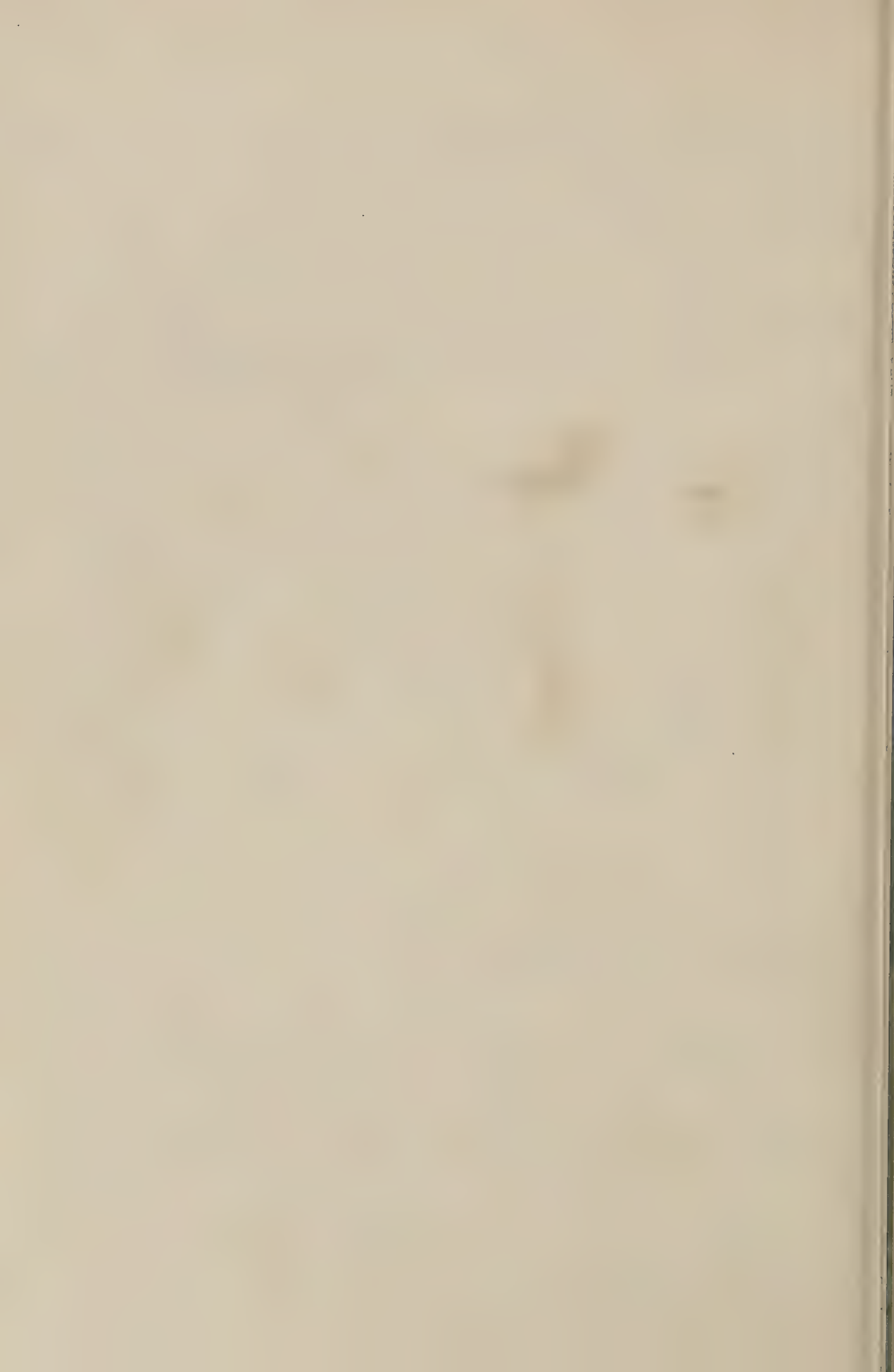
Réciproquement soit  $L$  un langage vérifiant les hypothèses ci-dessus. Alors pour tout élément  $m$  du monoïde syntactique  $M_L$  de  $L$  il existe des entiers naturels  $k$  et  $l$  tels que  $k \neq l$  et  $m^k = m^l$ . On en déduit (prop. 1, § 3, chap. II) que pour tout mot  $w \in X^*$ , il existe  $k$  et  $l$  comme ci-dessus tels que

$$\mu_S(w)^k - \mu_S(w)^l = 0$$

et  $\mu_S(w)$  est entier algébrique sur  $K$ . Il suffit alors d'appliquer le théorème de Chirchov.  $\square$

La condition (ii) du théorème 1 permet dans certains cas d'étendre au cas des séries en plusieurs variables des propriétés connues pour les séries d'une variable (cf. le chapitre suivant). Malheureusement, la condition (i) est souvent assez difficilement vérifiable. Nous allons préciser ce qu'elle signifie.





Proposition 1. Soit  $S$  une série rationnelle. Alors  $\mathcal{M}_S$  vérifie une identité polynômiale admissible si et seulement s'il existe un entier  $n$  et des coefficients  $a_\sigma$ ,  $\sigma \in \mathfrak{S}_n$ , dont l'un vaut 1, tels que

$$\forall a, u_1, \dots, u_n, b \in X^* \quad \sum_{\sigma \in \mathfrak{S}_n} a_\sigma (S, a u_{\sigma(1)} \dots u_{\sigma(n)} b) = 0$$

Preuve. La relation ci-dessus est exactement équivalente à

$$\forall u_1, \dots, u_n \in X^* \quad \sum_{\sigma} a_\sigma \mu_S(u_{\sigma(1)}) \dots \mu_S(u_{\sigma(n)}) = 0$$

Or les éléments  $\mu_S(w)$  ( $w \in X^*$ ) de  $\mathcal{M}_S$  engendrent  $\mathcal{M}_S$  comme  $K$ -module.

Comme le membre gauche de la relation précédente est multilinéaire, elle est équivalente à

$$\forall m_1, \dots, m_n \in \mathcal{M}_S \quad \sum_{\sigma} a_\sigma m_{\sigma(1)} \dots m_{\sigma(n)} = 0$$

Pour conclure, il suffit de remarquer qu'une algèbre vérifie une identité polynômiale admissible si et seulement si elle vérifie une identité multilinéaire (cf. § 2).  $\square$

Ce résultat peut encore être précisé dans le cas des séries rationnelles. Rappelons qu'on désigne par  $S_n$  le polynôme en les variables  $x_1, \dots, x_n$  :

$$S_n = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) x_{\sigma(1)} \dots x_{\sigma(n)}$$

où  $\varepsilon(\sigma)$  est la signature de  $\sigma$ .

Alors, si  $\mathcal{M}$  est une  $K$ -algèbre qui peut être engendrée, comme  $K$ -module, par  $n-1$  éléments,  $\mathcal{M}$  vérifie l'identité  $S_n = 0$ .

(cf. Procesi, chap. I, th. 3.20)

Par conséquent, la condition (i) du théorème peut être remplacée par

(i') Il existe  $n$  tel que

$$\forall a, u_1, \dots, u_n, b \in X^* \quad \sum_{\sigma} \varepsilon(\sigma) (S, a u_{\sigma(1)} \dots u_{\sigma(n)} b) = 0$$

Dans le cas des langages et du théorème 2, la condition pour  $\mathcal{M}_S$  de vérifier une identité polynômiale peut donc être remplacée par une condition plus maniable. Si  $L$  est un langage et  $a, u_1, \dots, u_n, b$  des mots soit  $n_p(L, a, u, b)$  (resp.  $n_I(L, a, u, b)$ ) le nombre de permutations paires (resp. impaires)  $\sigma$  telles que

$$a u_{\sigma(1)} \dots u_{\sigma(n)} b \in L.$$

La condition mentionnée devient alors :

$$\forall a, u_1, \dots, u_n, b \quad n_p(L, a, u, b) = n_I(L, a, u, b)$$

l'égalité pouvant même être remplacée par l'égalité modulo 2 (par exemple) si l'on prend pour  $K$  le corps à deux éléments.

Nous obtenons en particulier la

Proposition 2. Soit  $L$  un langage rationnel. Il existe un entier  $n$  tel que pour tous  $a, u_1, \dots, u_n, b \in X^*$

$$|\{\sigma \text{ pair} \mid a u_{\sigma(1)} \dots u_{\sigma(n)} b \in L\}| = |\{\sigma \text{ impair} \mid a u_{\sigma(1)} \dots u_{\sigma(n)} b \in L\}|$$

Nous avons mentionné que la condition (i) du théorème 1 était difficilement vérifiable. Il y a un cas cependant où elle est triviale : c'est le cas des séries et des langages échangeables.

Définition 2. Une série  $S$  (resp. un langage  $L$ ) est *échangeable* si pour tous mots  $a, u, v, b$  on a

$$(S, a u v b) = (S, a v u b)$$

$$(\text{resp. } a u v b \in L \Leftrightarrow a v u b \in L)$$

Autrement dit, le coefficient d'un mot dans  $S$  ne dépend que de son image commutative. Il est bien connu que le monoïde syntactique d'un langage échangeable est commutatif. De même, l'algèbre syntactique d'une série échangeable est commutative, comme il résulte immédiatement des définitions. Par conséquent, elle vérifie l'identité polynômiale.

$$xy - yx = 0$$

Dans ce cas particulier, le théorème 1 se formule de la manière suivante :

Théorème 3. Soit  $S$  une série formelle échangeable telle que pour toute lettre  $x \in X$  les séries d'une variable

$$\sum_{n \geq 0} (S, u x^n v) t^n \quad (u, v \in X^*)$$

vérifient une relation de récurrence linéaire commune. Alors  $S$  est rationnelle.

#### 4. RELATIONS DE RECURRENCE LINEAIRES BILATERES.

Dans ce paragraphe nous donnons, pour les idéaux de  $K\langle X \rangle$ , des ensembles générateurs particuliers, ce qui nous permet, par restriction aux idéaux syntactiques, de trouver des relations de récurrence linéaire bilatères pour les séries, distinctes de celles employées par Schützenberger (1961).

Nous supposons que  $K$  est un corps.

Nous avons besoin de quelques résultats élémentaires sur les ensembles ordonnés.

Soit  $E$  un ensemble ordonné dont l'ordre sera noté  $\leq$ . Un cône  $\mathcal{C}$  est une partie de  $E$  vérifiant

$$\forall u \in \mathcal{C}, \forall v \leq u, \quad v \in \mathcal{C}$$

Un anticône  $\mathcal{A}$  est une partie de  $E$  vérifiant

$$\forall u \in \mathcal{A}, \forall v \geq u, \quad v \in \mathcal{A}$$

Il est clair que le complémentaire d'un cône est un anticône et vice versa.

sailles. Nous parlerons de cône et d'anticône engendré par une partie de  $E$ . Nous supposons que toute partie non vide de  $E$  admet un élément minimal, appellerons code une partie  $C$  de  $E$  formée d'éléments deux à deux incomparables.

Lemme 1. Il y a bijection entre codes et cônes de  $E$ , de la manière suivante :  
(i) Si  $C$  est un code on lui associe le cône complémentaire de l'anticône engendré par  $C$ .

Si  $\mathcal{C}$  est un cône on lui associe le code des éléments minimaux du complémentaire de  $\mathcal{C}$ .

Preuve. (i) Soit  $C$  un code et  $\mathcal{C}$  le cône complémentaire de l'anticône engendré par  $C$ . Soit  $C'$  le code des éléments minimaux de  $E/\mathcal{C}$ .

- Si  $u \in C$ ,  $u \in E/\mathcal{C}$ . Soit  $v \in E/\mathcal{C}$  tel que  $v \subset u$ . Alors  $v$  est dans l'anticône engendré par  $C$  et il existe  $w \in C$  tel que  $w \subset v$ . Par suite  $w \subset u$ , donc  $w = u$  puisque les éléments de  $C$  sont deux à deux incomparables. Par suite  $w \subset v \subset u \Rightarrow v = u$  et  $u$  est un élément minimal de  $E/\mathcal{C}$ . Donc  $u \in C'$ .

- Si  $u \in C'$ ,  $u \in E/\mathcal{C}$  donc  $u$  est dans l'anticône engendré par  $C$  : il existe  $v \in C$  tel que  $v \subset u$ . Or,  $v \in E/\mathcal{C} \Rightarrow u = v \in C$ .

(ii) Soit  $\mathcal{C}$  un cône,  $C$  le code des éléments minimaux de  $E/\mathcal{C}$  et  $\mathcal{C}'$  le cône complémentaire de l'anticône engendré par  $C$ .

- Soit  $u \in \mathcal{C}$  : si  $v \subset u$ ,  $v \in \mathcal{C}$  donc  $v \notin C$ . Par suite  $u$  n'est pas dans l'anticône engendré par  $C$  donc  $u \in \mathcal{C}'$ .

- Soit  $u \in \mathcal{C}'$  : si  $u \notin \mathcal{C}$  soit  $v$  un élément minimal de l'ensemble  $F$  (non vide puisque  $u \in F$ )

$$F = \{ w \in E/\mathcal{C} \mid w \subset u \}$$

Alors  $v \in C$  ; en effet si  $w \in E/\mathcal{C}$  et  $w \subset v$ ,  $w$  est dans  $F$ , donc  $w = v$  par minimalité de  $v$ . Alors  $u$  est dans l'anticône engendré par  $C$  ce qui contredit  $u \in \mathcal{C}'$ .  $\square$

Nous appellerons *code puissant* un code  $C$  tel que le cône associé soit fini. Si  $u \in E$ , nous appelons *successeur* de  $u$  (resp. *prédécesseur* de  $u$ ) tout élément  $v \neq u$  tel que  $u \subset v$  (resp.  $v \subset u$ ) et tel que  $u \subset w \subset v$  (resp.  $v \subset w \subset u$ ) implique  $w = u$  ou  $w = v$ . Clairement, si  $u$  est prédécesseur de  $v$ ,  $v$  est successeur de  $u$ . Nous faisons l'hypothèse que  $E$  a un plus petit élément noté 1.

Lemme 2. La bijection du lemme 1, restreinte aux codes puissants, est une bijection entre codes puissants et cônes finis. De plus s'il existe  $\varphi: E \rightarrow \mathcal{P}(E)$ , une application associant à tout élément de  $E$  une partie de ses successeurs et telle que :

$$E = 1 \cup \bigcup_{u \in E} \varphi(u)$$

si  $C$  et  $\mathcal{C}$  sont en bijection

$$C \subset \varphi(\mathcal{C}) \quad \text{ou} \quad C = \{1\}.$$

Preuve. Soit  $C$  et  $\mathcal{C}$  en bijection. Clairement  $\mathcal{C}$  est fini, si  $C$  est puissant et réciproquement. Si  $\mathcal{C}$  est fini, soit  $\varphi$  comme dans l'énoncé et  $u \in C$ . Par hypothèse sur  $\varphi$  il existe  $v$  tel que  $u \in \varphi(v)$  (le cas  $C = \{1\}$  est trivial). Alors  $u \neq v$  et  $v \subset u$  donc  $v \in \mathcal{C}$ . Par suite,  $C \subset \varphi(\mathcal{C})$  et  $C$  est fini.  $\square$

Exemple 1 (i) Soit  $E = X$  et  $\in$  l'ordre préfixiel :  $u \subset v \Leftrightarrow v \in uX^*$ .

On retrouve alors la bijection classique entre codes préfixes et ensembles préfixiels. Un code puissant n'est alors autre qu'un code préfixe complet fini au sens classique (cf. chap. I, § 7).

(ii) Soit  $E = X^*$  et  $\in$  l'ordre des sous-mots : c'est l'ordre compatible avec la multiplication dans  $X^*$  qui est engendré par l'ordre préfixiel. Les codes sont alors les hypercodes au sens de Shyr et Thierrin (1974). Une des propriétés remarquables des hypercodes est qu'ils sont toujours finis (théorème de Higman, 1952)

(iii) Soit  $E = X^*$ , le monoïde commutatif libre engendré par  $X$  et  $\epsilon$  l'ordre

$$u \subset v \iff v \in u X^*.$$

Comme dans (ii) les codes obtenus sont toujours finis (théorème de Dickson cf. Eilenberg et Schützenberger, 1969).

Soit  $E = X^*$  et  $\subset$  l'ordre des facteurs :

$$u \subset v \iff v \in X^* u X^*.$$

Nous appellerons *code facteur* tout code pour l'ordre des facteurs et *code factoriel* tout cône pour cet ordre. Soit

$$\begin{aligned} \varphi: X^* &\rightarrow X^* \\ \varphi(u) &= u X \end{aligned}$$

Alors, d'après le lemme 2, si  $C$  et  $\mathcal{C}$  sont en bijection et  $C \neq 1$  on a

$$C \subset \mathcal{C}X$$

De manière plus précise

Lemme 3. Soient  $C \neq \{1\}$  un code facteur et  $\mathcal{C}$  un cône factoriel fini en bijection. On a  $C \subset \mathcal{C}X \setminus \mathcal{C}$ , avec égalité si et seulement si  $C$  est de la forme  $X^n$  ( $n \in \mathbb{N}$ ).

Preuve. Comme  $C \cap \mathcal{C} = \emptyset$  on a l'inclusion ci-dessus. Si  $C = X^n$ , alors  $\mathcal{C} = 1uXu \dots uX^{n-1}$  et  $C = \mathcal{C}X \setminus \mathcal{C}$ . Supposons  $C \neq \mathcal{C}X \setminus \mathcal{C}$ . Soit  $n$  la longueur maximum des mots dans  $\mathcal{C}$ . Soit  $xu \in C$  un mot de longueur  $n$  (avec  $x \in X$ ) : il en existe puisque si  $w \in \mathcal{C}$ ,  $|w| = n-1$ , on a  $wX \subset \mathcal{C}X \setminus \mathcal{C} = C$ . Soit  $y \in X$ , quelconque. On a  $u \in \mathcal{C}$  donc  $uy \in \mathcal{C}X$  et

$uy \notin \mathcal{C}$  puisque  $|uy| = n > n-1$ . Par suite  $uy \in C$ . On a donc établi :

$$xu \in C \cap X^n, y \in X \quad \wedge \quad uy \in C.$$

A partir de là, il n'est pas difficile de voir que  $C = X^n$ .  $\square$

Remarque 1. (Schützenberger). Si  $C$  est un code facteur fini, qui est maximal en tant que code au sens classique,  $C = X^n$ , pour un entier  $n$ . Il suffit de montrer que  $C = \mathcal{C}X\mathcal{C}$ . Mais, il existe  $u \in \mathcal{C}$  et  $x \in X$  tels que  $ux \notin \mathcal{C}$  et  $ux \in C$ , comme  $C$  est un code préfixe maximal, soit  $ux$  possède un facteur gauche dans  $C$ , soit  $ux$  est facteur gauche strict d'un mot de  $C$ ; dans le premier cas, soit  $ux \in C$ , ce qui n'est pas, soit  $u$  possède un facteur gauche dans  $C$ , ce qui n'est pas non plus, puisque  $u \in \mathcal{C}$ ; dans le second cas, on aurait  $ux \in \mathcal{C}$ .

Nous supposons dans la suite que  $X$  est *totale*ment ordonné et ordonnons  $X^*$  *lexicographiquement*. Notation :  $\leq$ ;  $w < w'$  si et seulement si

$$\text{soit } |w| < |w'|$$

$$\text{soit } |w| = |w'| \text{ et } w = uxv, w' = uyv'$$

$$x, y \in X \quad \text{et} \quad x < y.$$

Une remarque utile est la suivante :

$$- u \subset v \quad \Rightarrow \quad u < v$$

$$- u < v \quad \Rightarrow \quad aub < avb$$

Proposition 1. Soit  $\mathcal{J}$  un idéal de  $K\langle X \rangle$ . Il existe un couple  $(C, \mathcal{C})$ , formé d'un code facteur et du cône factoriel associé, et une famille  $\alpha_{u,f}$  ( $u \in C$ ,  $f \in \mathcal{C}$ ) d'éléments de  $K$  tels que les polynômes

$$u = \sum_{f \in \mathcal{C}} \alpha_{u,f} f, \quad u \in C$$

engendrent l'idéal  $\mathcal{J}$ , que :  $\alpha_{u,f} \neq 0$  implique  $f < u$  et que si  $\mathcal{J}$  est de codimension finie  $n$ ,

Preuve. Nous construisons une suite de mots

$$1 = f_1 < f_2 \dots < f_p < \dots$$

(finie ou infinie selon que  $\mathcal{J}$  est de codimension finie ou non) telle que

- Les  $f_i$  sont  $K$ -linéairement indépendants modulo  $\mathcal{J}$ .
- Si pour un  $i$ ,  $f_i < w < f_{i+1}$  alors ou bien  $w$  possède un facteur strict  $\notin \{f_1, \dots, f_i\}$  ou bien  $w$  est, modulo  $\mathcal{J}$ , combinaison linéaire des  $f_1, \dots, f_i$ .
- Si pour un  $i$ ,  $w \in f_i$ , alors  $w$  est dans la suite.

Ceci se fait de la manière suivante :

Nous posons  $f_1 = 1$ .

Supposons construits  $f_1, \dots, f_i$ .

Si pour tout mot  $w > f_i$ , ou bien  $w$  a un facteur strict  $\notin \{f_1, \dots, f_i\}$  ou bien  $w$  est combinaison linéaire, modulo  $\mathcal{J}$ , des  $f_1, \dots, f_i$ , nous posons  $i = p$  et la construction est terminée. Sinon il existe des mots  $w > f_i$  tel que tous les facteurs stricts de  $w$  sont dans  $\{f_1, \dots, f_i\}$  et que  $f_1, \dots, f_i$  <sup>sont</sup> indépendants modulo  $\mathcal{J}$ . Dans ce cas, nous prenons pour  $f_{i+1}$  le plus petit de ces mots (dans l'ordre lexicographique).

Si  $\text{codim}(\mathcal{J}) = n < \infty$ , la suite  $f_1, \dots, f_p$  obtenue vérifie  $p \leq n$ , il n'y a pas plus de  $n$  mots linéairement indépendants modulo  $\mathcal{J}$ .

Soit  $\mathcal{C}$  le cône factoriel  $\{f_1, \dots, f_i, \dots\}$  et  $C$  le code facteur des éléments minimaux de  $X^* \setminus \mathcal{C}$ .

Soit  $u \in C$ . Par construction, il existe alors des éléments  $\alpha_{u,f}$  ( $f \in \mathcal{C}$ ) de  $K$  tels que

$$u = \sum_{f \in \mathcal{C}} \alpha_{u,f} f \quad \text{mod. } \mathcal{J}$$

$$\alpha_{u,f} \neq 0 \Rightarrow f < u.$$

Posons :  $P_u = u - \sum_{f \in \mathcal{C}} \alpha_{u,f} f \quad (u \in C)$

Nous vérifions que pour tout mot  $w$  il existe des scalaires  $\alpha_f$  ( $f \in \mathcal{C}$ ) et des polynômes  $R_u, Q_u$  ( $u \in C$ ) tels que

$$w = \sum_{f \in \mathcal{C}} \alpha_f f + \sum_{u \in C} R_u P_u Q_u$$

et ceci par récurrence lexicographique.

C'est clair si  $w \in \mathcal{C}$  (en particulier si  $w = 1$ ).

De même, c'est clair si  $w = u \in C$ , car

$$u = P_u + \sum_{f \in \mathcal{C}} \alpha_{u,f} f$$

Soit  $w \in X^* \setminus \mathcal{C} \cup C$ .

Alors  $w$  s'écrit

$$w = aub, \quad u \in C, \quad ab \neq 1.$$

Alors

$$w = aP_u b + \sum_{\substack{f \in \mathcal{C} \\ f < u}} \alpha_{u,f} a f b$$

Or  $f < u \Rightarrow a f b < a u b = w$

On applique alors l'hypothèse de récurrence aux mots  $a f b$  et l'on peut conclure.

Par linéarité, on en déduit que pour tout polynôme  $P \in K\langle X \rangle$  il existe des

$\alpha_f \in K$  et des  $R_u, Q_u \in K\langle X \rangle$  tels que

$$P = \sum_{f \in \mathcal{C}} \alpha_f f + \sum_{u \in C} R_u P_u Q_u$$

Or,  $P_u \in \mathcal{J}$ , donc si  $P \in \mathcal{J}$

$$0 = \sum_{f \in \mathcal{C}} \alpha_f f \quad \text{mod. } \mathcal{J}$$

Or les  $f$  sont linéairement indépendants modulo  $\mathcal{J}$ , donc les  $\alpha_f$  sont nuls et

$$P = \sum_{u \in C} R_u P_u Q_u$$

Il suit de là que les  $P_u$  engendrent l'idéal  $\mathcal{J}$ .

Si  $\text{codim}(\mathcal{J}) = n < \infty$ , comme tout  $P \in K\langle X \rangle$  est égal modulo  $\mathcal{J}$  à une combinaison linéaire des  $f \in \mathcal{C}$ , il vient  $n \leq p \Rightarrow n = p$  et  $|\mathcal{C}| = n$ .  $\square$

Remarque 2. Le lecteur se convaincra aisément que si l'on sait calculer dans l'algèbre  $K\langle X \rangle / \mathcal{J}$  alors les constructions ci-dessus sont effectives.

Exemple 2. Soit  $\nu : \mathbb{Q}\langle x, y \rangle \rightarrow \mathbb{Q}^{2 \times 2}$

$$\nu x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \nu y = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

et posons  $\mathcal{J} = \text{Ker } \nu$ .

$\nu x^2$  est combinaison linéaire de  $\nu 1$  et  $\nu x$ , mais  $\nu xy = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$  est linéairement indépendant de  $\nu 1, \nu x, \nu y$ .

Comme  $\nu(\mathbb{Q}\langle x, y \rangle)$  est de dimension au plus 4, on a  $\text{codim}(\mathcal{J}) = 4$  et

$$\mathcal{C} = \{1, x, y, xy\}$$

Le code facteur  $\mathcal{C}$  est alors

$$\mathcal{C} = \{x^2, yx, y^2\}$$

et l'on a

$$\begin{aligned} x^2 &= 2x - 1 && \text{mod. } \mathcal{J} \\ yx &= 2x + 2y - xy - 1 && \text{mod. } \mathcal{J} \\ y^2 &= 2y - 1 && \text{mod. } \mathcal{J} \end{aligned}$$

donc les trois polynômes

$$x^2 - 2x + 1, xy + yx - 2x - 2y + 1, y^2 - 2y + 1$$

engendrent l'idéal  $\mathcal{J}$ .

Remarque 3. Une construction analogue s'applique aux idéaux à droite de  $K\langle X \rangle$  et permet de redémontrer un théorème de Cohn (1969, §2 (iv) et (v)) sur la liberté de ces idéaux. (voir aussi le § 7 du chapitre I, Schützenberger, 1961, III. B.1, Lewin 1969 et Reutenauer, 1978 a th. 6, § 4).

Cette méthode n'est d'ailleurs pas sans avoir quelques liens avec la méthode de Schreier pour démontrer la liberté des sous-groupes du groupe libre (cf. Lyndon et Schupp, 1977, prop. 3.7., chap. I).

Par ailleurs, elle s'applique aussi aux idéaux de  $K[X]$ , l'algèbre des polynômes en variables commutatives sur  $X$  : on prend comme relation d'ordre  $\subset$  celle qui est définie dans l'exemple 1 (iii) et comme relation  $\leq$  celle qui est définie comme suit sur le monoïde commutatif libre  $X^{\circ} = \mathbb{N}^X$  :

si  $u = (n_x)$ ,  $v = (m_x) \in \mathbb{N}^X$  alors  $u < v$  si et seulement si soit  $\sum n_x < \sum m_x$ , soit  $\sum n_x = \sum m_x$  et il existe  $x_0 \in X$  tel que  $x < x_0$  implique  $n_x = m_x$  et  $n_{x_0} < m_{x_0}$ .

Or (voir l'exemple cité) un code pour  $\subset$  est toujours fini. On retrouve ainsi que tout idéal de  $K[X]$  est de type fini. Cette construction s'adapte aussi aux congruences de  $X^{\circ}$  (voir Sakarovitch, 1978, th. 2) et permet de retrouver que toute congruence de  $X^{\circ}$  est de type fini (Redei, 1965).

Théorème 1. Soit  $S \in K\langle\langle X \rangle\rangle$  une série rationnelle avec  $\dim(\mathcal{M}_S) = n$ . Il existe un couple  $(C, \mathcal{C})$  formé d'un code facteur puissant fini et d'un cône factoriel de cardinal  $n$  en bijection et une famille  $\alpha_{u,f}$  ( $u \in C$ ,  $f \in \mathcal{C}$ ) d'éléments de  $K$  tels que

- Pour tous mots  $a, b \in X^*$  et  $u \in C$

$$(S, aub) = \sum_{f \in \mathcal{C}} \alpha_{u,f} (S, afb)$$

-  $\alpha_{u,f} \neq 0 \Rightarrow f < u$ .

Preuve. Il suffit d'appliquer la proposition 2 à l'idéal syntactique de qui est de codimension  $n$ .  $\square$

## 5. SERIES RATIONNELLES CENTRALES

Rappelons que deux mots  $u$  et  $v$  sont dits *conjugués* s'il existe des mots  $a$  et  $b$  tels que  $u = ab$  et  $v = ba$ . On montre que deux mots sont conjugus si et seulement s'ils sont conjugus dans le groupe libre engendré par l'alphabet sur lequel ils sont écrits.

Définition 1. (i) Une série formelle  $S \in K \langle\langle X \rangle\rangle$  est dite *centrale* si pour tout couple de mots conjugus ces deux mots ont même coefficient dans

(ii) Une série formelle  $S \in K \langle\langle X \rangle\rangle$  est un *caractère* s'il existe un homomorphisme  $\mu : X^* \rightarrow K^{n \times n}$  tel que

$$\forall w \in X^*, \quad (S, w) = \text{Tr}(\mu w)$$

Remarque 1. Il est clair que tout caractère est une série rationnelle et centrale. La même chose est vraie pour les combinaisons linéaires de caractère. Toute série rationnelle centrale n'est cependant pas une combinaison linéaire de caractères, comme nous allons le voir. Cependant, lorsque  $K$  est un corps algébriquement clos de caractéristique 0, il est bien connu que toute fonction centrale d'un groupe fini dans  $K$  est une combinaison linéaire de caractères (voir Herstein, 1968, th. 5. 1.3).

Lemme 1. Soit  $S$  une série centrale.

$$(i) \quad \forall P, Q \in K \langle X \rangle, \quad (S, PQ) = (S, QP)$$

$$(ii) \quad \forall m, n \in M_S, \quad \varphi_S(mn) = \varphi_S(nm)$$

Preuve. On a :  $\forall u, v \in X^* \quad (S, uv) = (S, vu)$  et (i) s'en déduit par linéarité. De plus (ii) est conséquence immédiate de (i).  $\square$

Proposition 1. Soit  $S$  une série centrale. Alors l'idéal syntactique gauche de  $S$  est égal à son idéal syntactique.

Preuve. On a par définition  $\mathcal{I}_S \subset \mathcal{I}_S^g$ . Soit  $P \in \mathcal{I}_S^g$  : alors pour tout  $Q \in K\langle X \rangle$ ,  $(S, QP) = 0$  (lemme 2, § 2, chap. II). Par suite  $\forall Q, R \in K\langle X \rangle$   
 $(S, QPR) = (S, RQP) = 0$  (lemme 1).

Donc  $P \in \mathcal{I}_S$ .  $\square$

Remarque 2. On montre aisément qu'une algèbre de dimension finie est une algèbre de Frobenius (Curtis-Reiner, 1962, § 61) si et seulement si elle est l'algèbre syntactique d'une série rationnelle dont l'idéal syntactique est égal à l'idéal syntactique gauche (donc à l'idéal syntactique droit).

Théorème 1. On suppose que  $K$  est un corps. Soit  $S$  une série rationnelle.

(i) Si  $S$  est combinaison linéaire de caractères,  $\mathcal{M}_S$  est une algèbre semi-simples.

(ii) Si  $\mathcal{M}_S$  est semi-simple et  $K$  algébriquement clos,  $S$  est combinaison linéaire de caractères.

Preuve. (i) Il existe un entier  $r$ , des homomorphismes  $\mu_i : K\langle X \rangle \rightarrow K^{n_i \times n_i}$  et des  $a_i \in K$  tels que

$$\forall w \in X^*, (S, w) = \sum_{1 \leq i \leq r} a_i \operatorname{Tr}(\mu_i w)$$

Soit  $\mu : K\langle X \rangle \rightarrow \prod_i K^{n_i \times n_i}$

$$\mu = (\mu_1, \dots, \mu_r)$$

et  $\mathcal{M} = \mu(K\langle X \rangle)$ . Par ailleurs, soit

$$\varphi : \mathcal{M} \rightarrow K$$

$$\varphi(m_1, \dots, m_r) = \sum a_i \operatorname{Tr}(m_i)$$

Alors  $(M, \mu, \varphi)$  est une représentation surjective de  $S$ . Par suite, (th. 1, § 1, chap. II) il existe un idéal  $J$  de  $M$  tel que

$$M_S \simeq M/J$$

Soit  $R$  le radical (de Jacobson) de  $M$ . Alors  $R$  est nilpotent (Herstein 68, th. 1.3.1.) donc si  $m = (m_1, \dots, m_r) \in R$ , les  $m_i$  sont nilpotents, donc  $\text{Tr}(m_i) = 0 \Rightarrow \varphi(m) = 0$ . Par suite  $R$  est un idéal contenu dans  $\text{Ker } \varphi$ , donc dans  $J$ , sinon  $\text{Ker } \varphi_S$  contiendrait un idéal non nul (lemme 3, § 1, chap. II). Par suite  $M_S$  est quotient de  $M/R$ , donc semi-simple puisque  $M/R$  l'est (ibid. th. 1.4.4).

(ii)  $M_S$  est isomorphe à un produit de la forme

$$\prod_{1 \leq i \leq r} K^{n_i \times n_i}$$

(ibid. th. 2.1.8).

Si  $m_1, m_2 \in M_S$   $\varphi_S(m_1 m_2) = \varphi_S(m_2 m_1)$  (lemme 1).

Soit  $\varphi_i$  la restriction de  $\varphi_S$  à  $K^{n_i \times n_i}$  : il existe alors  $a_i \in K$  tel que

$$\varphi_i = a_i \text{Tr}$$

(En effet, si  $\psi$  est une forme linéaire sur  $K^{n \times n}$  telle que  $\psi(mm') = \psi(m'm)$ , il existe  $a \in K$  tel que  $\psi = a \text{Tr}$ , comme on le vérifie aisément).

Soit  $\mu_i$  la projection de  $\mu_S$  sur  $K^{n_i \times n_i}$ . Alors  $\forall w \in X^*$

$$(S, w) = \varphi \circ \mu_S(w) = \varphi(\mu_1 w, \dots, \mu_r w) = \sum_{1 \leq i \leq r} a_i \text{Tr}(\mu_i w) \quad \square$$

Nous donnons maintenant une caractérisation de certaines séries rationnelles centrales, répondant ainsi à une question de Fliess (1972, appendice)

Théorème 2. On suppose que  $K$  est un corps algébriquement clos. Soit  $S$  une série rationnelle de  $K\langle\langle X \rangle\rangle$  telle que  $(S, 1) = 1$ . Alors  $S$  est centrale si et seulement s'il existe une représentation linéaire réduite de  $S$   $(\lambda, \nu, \gamma)$  avec  $\lambda = (1, 0, \dots, 0)$ ,  $\gamma = {}^t\lambda$  et où  $\nu : X^* \rightarrow K^{n \times n}$  vérifie :

$$\forall w \in X^*, \forall i \in \{1, \dots, n\} \quad (\nu w)_{1,i} = (\nu w)_{i,1}$$

Remarque 3. Avec  $\lambda, \nu, \gamma$  comme ci-dessus, on a  $(S, w) = \lambda \nu w \gamma = (\nu w)_{1,1}$

Preuve. La condition est clairement suffisante puisque

$$\begin{aligned} (S, uv) &= (\nu uv)_{1,1} = \sum_{1 \leq i \leq n} (\nu u)_{1,i} (\nu v)_{i,1} \\ &= \sum (\nu v)_{1,i} (\nu u)_{i,1} = (\nu v u)_{1,1} = (S, vu) \end{aligned}$$

Pour la réciproque nous nous inspirons de techniques utilisées dans l'étude des algèbres symétriques (Curtis-Reiner, 1962, § 66). Rappelons qu'une représentation linéaire réduite de  $S$  est une représentation de dimension minimum de  $S$  et que cette dimension est égale au rang de  $S$  et aussi à la dimension du module sériel réduit de  $S$  (Fliess, 1974, chap. II, § 1). Or, cette dimension est égale à celle de  $K\langle X \rangle / \mathcal{I}_S^g$  (prop. 1, § 2. chap. II) donc à celle de  $\mathcal{M}_S$ , si  $S$  est centrale (proposition 1).

Posons  $\dim(\mathcal{M}_S) = p$  et soit  $B$  la forme bilinéaire sur  $\mathcal{M}_S$

$$B(m, n) = \varphi_S(mn)$$

$B$  est symétrique (lemme 1) et non dégénérée : en effet le noyau de  $B$

$$\text{Ker } B = \{ m \mid \forall n, \varphi_S(mn) = 0 \}$$

est clairement un idéal à droite, donc aussi un idéal à gauche puisque

$$\varphi_S(mn) = \varphi_S(nm). \text{ Par suite } \text{Ker } B \text{ est un idéal contenu dans } \text{Ker } \varphi,$$

donc  $\text{Ker } B = 0$  (lemme 3, § 1. chap. II).

Comme  $K$  est algébriquement clos, il existe une base  $m_1, \dots, m_p$  de  $\mathcal{M}_S$  orthonormale pour  $B$ . On peut même supposer  $m_1 = 1$ , puisque  $B(1, 1) = (S, 1) = 1$ .

$$\text{On a } \forall i, j \quad B(m_i, m_j) = \delta_{i,j} = \varphi_S(m_i m_j)$$

$$\text{et en particulier } B(m_1, m_j) = \delta_{1,j} = \varphi_S(m_j).$$

Pour tout  $m \in \mathcal{M}_S$  il existe des matrices  $\bar{\nu}(m) \in K^{p \times p}$  telles que

$$\forall i \in \{1, \dots, p\} \quad m_i m = \sum_{1 \leq j \leq p} \bar{\nu}(m)_{i,j} m_j$$

L'application  $\bar{\nu} : \mathcal{M}_S \rightarrow K^{p \times p}$  ainsi définie est un homomorphisme d'algèbres (c'est la représentation régulière droite de  $\mathcal{M}_S$ ). De plus :

$$\varphi_S(m_i m) = \varphi_S\left(\sum_j \bar{\nu}(m)_{i,j} m_j\right) = \bar{\nu}(m)_{i,1}$$

$$\varphi_S(m m_i) = \varphi_S(m_1 m m_i) = \varphi_S\left(\sum_j \bar{\nu}(m)_{1,j} m_j m_i\right) = \bar{\nu}(m)_{1,i}$$

$$\text{donc :} \quad \bar{\nu}(m)_{i,1} = \bar{\nu}(m)_{1,i}$$

Par ailleurs :

$$m = m_1 m = \sum_j \bar{\nu}(m)_{1,j} m_j \Rightarrow \varphi_S(m) = \bar{\nu}(m)_{1,1}$$

Soit  $\gamma : X^* \rightarrow K^{p \times p}$  défini par

$$\gamma w = \bar{\nu} \circ \mu_S(w)$$

$$\text{Alors } (\gamma w)_{1,1} = \bar{\nu}(\mu_S(w))_{1,1} = \varphi_S \circ \mu_S(w) = (S, w)$$

$$\text{et } (\gamma w)_{i,1} = (\gamma w)_{1,i} \quad \forall i \in \{1, \dots, p\}.$$

Alors  $(\lambda, \gamma, \gamma)$  (avec  $\lambda$  et  $\gamma$  comme dans l'énoncé) est une représentation linéaire de  $S$  de dimension  $p$  donc réduite.  $\square$

Exemple 1. Soit  $S = \sum_{n \geq 0} (n+1) x^n \in \mathbb{C}[[x]]$

Alors  $S$  admet la représentation linéaire

$$\mu_x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \lambda = (1, 0) \quad \gamma = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

qui est réduite. Par suite, l'algèbre syntactique de  $S$  est isomorphe à l'algèbre des matrices de la forme  $\left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in \mathbb{C} \right\}$

qui n'est pas semi-simple, puisqu'elle contient l'idéal nilpotent des matrices de la forme  $\left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \mid b \in \mathbb{C} \right\}$

Par suite  $S$  n'est pas combinaison linéaire de caractères (th. 1). Mais  $S$  admet une représentation linéaire réduite conforme au th. 2, à savoir

$$\nu_x = \begin{pmatrix} 2 & i \\ i & 0 \end{pmatrix}$$

(où  $i^2 = -1$ ).

Remarque 4. L'hypothèse "K-algébriquement clos" dans le th. 4 peut être remplacée par "K contient la racine carrée de chacun de ses éléments". En effet, cela suffit à assurer l'existence d'une base orthonormale pour les formes bilinéaires non dégénérées.

Dans le cas général (K corps quelconque) on obtient cependant l'énoncé suivant dont la preuve est analogue (on remplace la base orthonormale par une base orthogonale) :

Soit  $S$  une série rationnelle telle que  $(S, 1) \neq 0$ . Alors  $S$  est centrale si et seulement si elle possède une représentation linéaire réduite  $(\lambda, \nu, \gamma)$  avec

$$\lambda = (1, 0, \dots, 0) \quad \gamma = (S, 1)^t \lambda$$

et où  $\nu$  vérifie : il existe des scalaires  $a_1 = (S, 1), a_2, \dots, a_n$  non nuls

tels que

$$\forall w, \forall i \quad (\nu w)_{l,i} a_i = (\nu w)_{i,l} a_l$$

Remarque 5. Il n'est pas difficile de montrer qu'une algèbre de dimension finie est symétrique (Curtis-Reiner, 1962, § 66) si et seulement si elle est l'algèbre syntactique d'une série rationnelle centrale.

Remarque 6. On peut trouver dans Choffrut (1978, chap. IV) des résultats sur les fonctions rationnelles centrales d'un monoïde libre dans un autre.

## CHAPITRE IV - APPLICATIONS

-----

Nous utilisons les résultats du paragraphe précédent pour étendre aux séries rationnelles en plusieurs variables non commutatives des résultats classiques pour celles d'une variable. Il s'agit d'une part du problème des extensions de Fatou, posé par Benzaghou et Fliess ; nous généralisons des résultats de Cahen et Chabert (§ 1). L'autre problème est celui du quotient de Hadamard, posé par Pisot, et sur lequel se sont penchés nombre de chercheurs (§ 2). Pour des détails et un bref historique, le lecteur se reportera aux introductions des deux paragraphes.

# 1. EXTENSIONS DE FATOU.

P. Fatou (1904) a démontré le résultat suivant, connu sous le nom de lemme de Fatou :

*Soient  $P, Q$  deux polynômes premiers entre eux en une variable à coefficients dans  $\mathbb{Z}$  tels que  $Q(0) \neq 0$ . Si les coefficients du développement en série de la fraction rationnelle  $P/Q$  sont tous entiers, alors  $Q(0) = 1$ .*

Cette propriété a été étendue au cas d'autres anneaux que  $\mathbb{Z}$  par Benzaghou (1970) qui a montré que de tels anneaux sont nécessairement complètement intégralement clos et Chabert (1972) a montré que cette condition est aussi suffisante. Une propriété analogue pour les séries en plusieurs variables a conduit Fliess (1974) à définir les anneaux de Fatou forts : il montre que les anneaux principaux sont de tels anneaux, et Sontag et Rouchaleau (1977) montrent que si  $A$  est principal,  $A[[t]]$  est un anneau de Fatou fort. Une caractérisation complète des anneaux de Fatou forts fait toujours défaut.

En même temps, Fliess définit les extensions de Fatou : un demi-anneau  $B$  est une extension de Fatou du demi-anneau  $A$  si toute série  $B$ -rationnelle à coefficients dans  $A$  est  $A$ -rationnelle. Pour des exemples d'extensions de Fatou, on peut consulter Salomaa-Soittola (1977, chap. II, § 6). La propriété analogue pour les séries d'une variable a été étudiée par Cahen et Chabert (1975) qui ont caractérisé les extensions d'anneaux intègres ayant cette propriété. Nous montrons ici que leur caractérisation est encore valable pour les séries en plusieurs variables non commutatives.

Définition 1. Soit  $A \subset B$  deux demi-anneaux.  $B$  est extension de Fatou de  $A$  si toute série  $B$ -rationnelle à coefficients dans  $A$  est  $A$ -rationnelle.

Nous fixons dans la suite un anneau commutatif  $A$  avec corps de fractions

Définition 2. Soit  $x$  un élément d'une  $K$ -algèbre.  $x$  est *quasi-entier* sur  $A$  si le  $A$ -module  $A[x]$  peut s'injecter dans un  $A$ -module de type fini.

Lemme 1. (Cahen-Chabert, 1975). Soit  $B$  un sur-anneau commutatif intègre de  $A$ .

(i) L'ensemble des éléments de  $B$  qui sont quasi-entiers sur  $A$  est un sous-anneau de  $B$ .

(ii)  $x \in K$  est quasi-entier sur  $A$  si et seulement s'il existe  $d \in A/O$  tel que

$$\forall n \in \mathbb{N}, \quad dx^n \in A.$$

Lemme 2. Soit  $m \in K^{p \times p}$  une matrice, où  $K$  est le corps des fractions de l'anneau commutatif  $A$ . On suppose qu'il existe  $d \in A/O$  tel que  $\forall n \in \mathbb{N}$ ,  $dm^n \in A^{p \times p}$ . Alors les valeurs propres de  $m$  sont quasi-entières sur  $A$ .

Ce lemme est démontré dans Reutenauer (1978).  $\square$

Corollaire. Soit  $M$  une  $K$ -algèbre et  $x \in M$  quasi-entier sur  $A$ . Alors  $x$  est algébrique sur  $K$  et les coefficients du polynôme minimal de  $x$  sur  $K$  sont quasi-entiers sur  $A$ .

Preuve. Soit  $M$  un  $A$ -module de type fini et  $A[x] \rightarrow M$  une injection  $A$ -linéaire. Comme  $A[x]$  est sans torsion, puisque contenu dans une  $K$ -algèbre, cette injection se prolonge en une injection  $K$ -linéaire  $i : K[x] \rightarrow M \otimes_A K$  donc  $K[x]$  est de dimension finie sur  $K$  et  $x$  est algébrique. Soit  $p : M \otimes_A K \rightarrow i(K[x])$  une projection  $K$ -linéaire. Alors  $p(M) = p(M \otimes_A i)$  est un  $A$ -module de type fini contenant  $i(A[x])$  et contenu dans  $i(K[x])$ . Par suite, son image réciproque  $M_1$  est un  $A$ -module de type fini et  $A[x] \subset M_1 \subset K[x]$ .

Soit  $\mu : K[x] \rightarrow K^{p \times p}$  un homomorphisme injectif de  $K$ -algèbres :  $\mu(M_1)$  est un  $A$ -module de type fini, donc il existe  $d \in A/O$  tel que  $d \mu(M_1) \subset A^{p \times p}$ . Or,  $\forall n \in \mathbb{N}$ ,  $x^n \in M_1$  donc  $d \mu x^n \in A^{p \times p}$ . D'après le lemme 2, les valeurs propres de  $\mu x$  sont quasi-entières sur  $A$  et d'après

le lemme 1 (i), les coefficients du polynôme minimal de  $\mu x$ , donc de  $x$ , le sont aussi.  $\square$

Lemme 3. Soit  $S$  une série  $K$ -rationnelle à coefficients dans  $A$  et  $(\mathbb{M}, \mu, \varphi)$  la  $K$ -représentation minimale de  $S$ , Soit  $\mu'$  la restriction de  $\mu$  à  $A\langle X \rangle$ ,  $\mathbb{M}' = \mu(A\langle X \rangle)$  et  $\varphi'$  la restriction de  $\varphi$  à  $\mathbb{M}'$ . Alors  $(\mathbb{M}', \mu', \varphi')$  s'identifie à la  $A$ -représentation minimale de  $S$  et il existe un  $A$ -module de type fini  $M$  tel que  $\mathbb{M}' \subset M \subset \mathbb{M}$ .

Preuve. Comme pour tout  $P \in A\langle X \rangle$

$$\varphi \circ \mu(P) = \sum_{w \in X^*} (P, w) \varphi \circ \mu(w) = \sum (P, w) (S, w) \in A$$

$(\mathbb{M}', \mu', \varphi')$  est une  $A$ -représentation de  $S$ .

De plus, si  $P$  est dans l'idéal syntactique de  $S$  sur  $A$ , on a :

$$\forall Q, R \in A\langle X \rangle, \quad (S, QPR) = 0$$

donc la même relation est vraie si  $Q, R \in K\langle X \rangle$ . Par suite,  $P$  est dans l'idéal syntactique de  $S$  sur  $K$ , i.e.  $\text{Ker } \mu$ . Donc  $(\mathbb{M}', \mu', \varphi')$  s'identifie à la  $A$ -représentation minimale de  $S$ .

Pour la dernière assertion, il suffit d'utiliser le théorème 2 du chap. III, § 1 et le corollaire 1 au théorème 1, § 3, chap. I.  $\square$

Théorème 1. Soit  $B$  un sur-anneau commutatif intègre de  $A$ . Alors  $B$  est extension de Fatou de  $A$  si et seulement si tout  $x \in K$ , quasi-entier sur  $A$  et entier sur  $B$ , est entier sur  $A$ .

Preuve. La nécessité de la condition découle des travaux de Cahen et Chabert (1975). Réciproquement, supposons que tout  $x \in K$ , entier sur  $B$  et quasi-entier sur  $A$ , est entier sur  $A$ . Soit  $S$  une série  $B$ -rationnelle à coefficients dans  $A$ . Soit  $L$  le corps des fractions de  $K$ . Alors  $S$  est  $L$ -rationnelle à coefficients dans  $K$ , donc  $K$ -rationnelle (corollaire 3 à la prop. 3, § 3,

chap. I). Soit  $(\mathbb{M}, \mu, \psi)$  et  $(\mathbb{M}', \mu', \psi')$  comme dans le lemme 3 ;

$\mathbb{M}$  vérifie une identité polynômiale à coefficients 1 et -1 (Procesi 1973,

th. 1, 3.20) et il en est donc de même pour  $\mathbb{M}'$ .

D'après le lemme 3, tout élément de  $\mathbb{M}'$  est quasi-entier sur  $A$ , donc d'après le lemme 2, algébrique sur  $K$  et les coefficients de son polynôme minimal sur  $K$  sont quasi-entiers sur  $A$ .

$S$  est  $B$ -rationnelle et admet donc une  $B$ -représentation finie et surjective  $(\mathbb{M}_1, \mu_1, \psi_1)$ . Alors, d'après la prop. 1 du § 4, chap. II  $(\mathbb{M}_1 \otimes_B L, \mu_1 \otimes_B \text{id}, \psi_1 \otimes_B \text{id})$  est une  $L$ -représentation surjective de  $S$  et d'après la prop. 2 du § 2, chap. II  $(\mathbb{M} \otimes_K L, \mu \otimes_K L, \psi \otimes_K L)$  s'identifie à la  $L$ -représentation minimale de  $S$ . Par suite (th. 1, § 1, chap. II), il existe un homomorphisme surjectif  $\gamma$  de  $L$ -algèbres tel que le diagramme suivant soit commutatif

$$\begin{array}{ccc}
 & L\langle X \rangle & \\
 \mu_1 \otimes \text{id} \swarrow & & \searrow \mu \otimes \text{id} \\
 \mathbb{M}_1 \otimes_B L & \xrightarrow{\gamma} & \mathbb{M} \otimes_K L
 \end{array}$$

Soit  $m \in \mathbb{M}'$ . Il existe alors  $P \in A\langle X \rangle$  tel que  $m = \mu(P)$ . Alors

$\mu_1(P) \in \mathbb{M}_1$  est entier sur  $B$ , donc  $m \otimes 1$  est entier sur  $B$ . Par suite,

les racines du polynôme minimal de  $m \otimes 1$  sur  $L$  sont entières sur  $B$ , et

il en est de même de ses coefficients. Or  $m$  est algébrique sur  $K$  et le poly-

nomme minimal de  $m$  sur  $K$  est égal à celui de  $m \otimes 1$  sur  $L$ . Par suite,

ses coefficients sont entiers sur  $B$  et, comme nous l'avons vu, quasi-entiers

sur  $A$ , donc entiers sur  $A$ . On en déduit que  $m$  est entier sur  $A$ . Il s'af-

fit alors d'appliquer le théorème de Chirchov (§ 2, chap. III) pour en conclure

que  $\mathbb{M}'$  est un  $A$ -module de type fini.  $\square$

Définition 3.  $A$  est un anneau de Fatou faible si  $K$  est extension de Fatou de  $A$ .

Le théorème 1 a la conséquence suivante :

Théorème 2.  $A$  est un anneau de Fatou faible si et seulement si tout  $x \in A$  qui est quasi-entier sur  $A$ , est aussi entier sur  $A$ .

Remarque 1. On peut démontrer le résultat suivant (Reutenauer, 1977, th. 1, chap. III) :

$A$  est un anneau de Fatou faible si et seulement si pour toute  $K$ -algèbre  $M$  toute sous- $A$ -algèbre de type fini  $M'$  de  $M$  qui est contenue dans un sous-module de type fini de  $M$ ,  $M'$  est un  $A$ -module de type fini.

Remarque 2. (i) Il existe des anneaux qui ne sont pas des anneaux de Fatou faibles, voir Bourbaki (1961, chap. 5, exercice 2).

(ii) Les anneaux noethériens sont des anneaux de Fatou faibles car ils vérifient la condition du théorème 2, voir Bourbaki (1961, chap. 5, § 1, n° 1 corollaire à la proposition 1).

(iii) Il en est de même des anneaux complètement intégralement clos, et en particulier des anneaux factoriels.

## 2. UN QUOTIENT DE HADAMARD

Polya (1921) a montré que si une primitive de la fonction rationnelle  $\sum a_n x^n$  à coefficients dans  $\mathbb{Z}$  a encore ses coefficients dans  $\mathbb{Z}$ , alors cette primitive est encore une fonction rationnelle.

Ce résultat peut se formuler autrement : si  $S, T$  sont des séries formelles, rappelons que le produit de Hadamard de  $S$  et de  $T$  est la série  $S \odot T$  définie par

$$(S \odot T, w) = (S, w) (T, w)$$

On sait que le produit d'Hadamard de deux séries rationnelles est encore une série rationnelle (dans le cas des séries en plusieurs variables ce théorème a été démontré par Schützenberger, 1962). La réciproque est fautive : la série

$$\sum \frac{t^n}{n+1}$$

qui est quotient d'Hadamard de  $\sum t^n$  par  $\sum (n+1)t^n$  n'est pas rationnelle. Le résultat de Polyá ci-dessus dit cependant que si le quotient d'Hadamard de la série rationnelle  $\sum a_n t^n$  par  $\sum (n+1)t^n$  est à coefficients entiers, alors ce quotient est une série rationnelle. Ce résultat a été étendu par Cantor (1965) au cas où  $a_n$  est un polynôme en  $n$ , par Pisot (1959) et Benzaghou (1970) au cas où le polynôme exponentiel associé à  $(a_n)$  a un pôle dominant (ce qu'on exprime en disant que  $(a_n)$  est une suite de Pisot) et par Pathiaux (1968) au cas où ce polynôme a exactement deux pôles dominants...

Par ailleurs, Lamèche (1973) et Jacob (197X) ont étudié le cas du quotient d'Hadamard d'une série rationnelle en plusieurs variables par la série

$$\sum_{w \in X^*} (|w| + 1) w$$

Notre travail, dans ce paragraphe, consiste à généraliser les résultats de Lamèche et Jacob, en utilisant le critère de rationalité du théorème 1, chap. III, § 3.

La difficulté est triple :

appelons  $S$  et  $T$  deux séries rationnelles dont le quotient d'Hadamard  $U$  est à coefficients entiers.

- La condition " $\mathcal{M}_U$  vérifie une identité polynômiale" ne s'obtient pas en général comme conséquence du fait que  $\mathcal{M}_S$  et  $\mathcal{M}_T$  sont rationnelles. C'est pourquoi nous supposons que  $T$  est échangeable (i.e. que si deux mots ont même image commutative alors ils ont même coefficient dans  $T$ ) : ceci assure que  $\mathcal{M}_U$  vérifie une identité polynômiale.

- Pour pouvoir appliquer les résultats concernant les quotients d'Hadarnard des séries d'une variable, il nous faut nous assurer que les séries  $T(R)$  associées aux rayons  $R$  font partie d'une classe de séries d'une variable pour lesquels on a des résultats positifs. Nous obtenons ce fait en exigeant que  $T$  soit à croissance polynômiale ou bien que  $T$  soit  $R_+$ -rationnelle ; en effet, une série  $R_+$ -rationnelle d'une variable est, à peu de choses près, une suite de Pisot (Berstel, 1971).

- Pour obtenir une relation de récurrence uniforme pour toutes les séries associées aux rayons de même période, nous avons dû démontrer un lemme, très technique, qui dit à peu près la chose suivante : étant donné une "relation de récurrence linéaire", toute série qui est à la fois rationnelle et quotient d'Hadarnard de deux séries vérifiant cette relation, cette série vérifie une certaine relation qui ne dépend que de la relation de départ.

Définition 1. Une série formelle  $S \in R\langle\langle X \rangle\rangle$  est à *croissance polynômiale* s'il existe  $a, b \geq 0$ , tels que  $\forall w \in X^+, |(S, w)| \leq a |w|^b$ .

Remarque 1. On montre qu'une série rationnelle  $S \in R\langle\langle X \rangle\rangle$  est au plus à *croissance exponentielle*, i.e. il existe  $a \geq 0$  tel que  $\forall w \in X^+, |(S, w)| \leq a^{|w|}$ .

Théorème 1. Soient  $S, T \in Z\langle\langle X \rangle\rangle$ . On suppose que  $S$  et  $T$  sont rationnelles, que  $T$  est échangeable et que pour tout  $w \in X^*, (S, w) / (T, w) \in Z$ . Si  $T$  vérifie au moins l'une des deux conditions suivantes :

- (i)  $T$  est à croissance polynômiale
- (ii)  $T$  est  $R_+$ -rationnelle

la série quotient d'Hadarnard de  $S$  par  $T$  est  $Z$ -rationnelle.

Le lemme qui suit concerne les séries rationnelles d'une variable (cf. chapitre 1)





Lemme 1. Soient  $K$  un corps commutatif de caractéristique nulle et  $P, Q \in K[x]$ , non nuls. Il existe un polynôme  $R \in K[x]$  vérifiant : pour toutes les séries  $S = \sum a_n x^n$  et  $T = \sum b_n x^n$  telles que  $P \circ S = 0$ ,  $Q \circ T = 0$  et que la série  $U = \sum (a_n / b_n) x^n$  est rationnelle, on a  $R \circ U = 0$ .

Nous démontrons ce lemme à la fin du paragraphe.

Preuve du théorème 1. Nous appliquons le critère du théorème 1, § 3, chap. III, avec  $K = Q$ .

(i)  $\mathcal{H}_S$  vérifie une identité polynômiale. Soit  $T'$  la série inverse d'Hadamard de  $T$

$$T' = \sum_w (T, w)^{-1} w$$

$T'$  est échangeable donc son algèbre syntactique est commutative. On vérifie aisément que la série  $U$  quotient d'Hadamard de  $S$  par  $T$  est reconnue par

$\mathcal{H}_S \otimes \mathcal{H}_{T'}$ . En effet

$$U = S \otimes T'$$

Or  $\mathcal{H}_S \otimes \mathcal{H}_{T'}$  vérifie une identité polynômiale (Procesi 73, chap. I, prop.

3.13) donc il en est de même pour  $\mathcal{H}_U$ .

(ii) Soient  $(\lambda, \nu, \gamma), (\lambda', \nu', \gamma')$  les représentations linéaires réduites de  $S$  et  $T$  respectivement. Soient  $w \in X^*$  et  $P$  le polynôme caractéristique de  $\gamma w$ ,  $Q$  celui de  $\gamma' w$ . Soit  $R$  le polynôme donné dans le lemme 1. Si  $u, v$  sont des mots dans  $X^*$ , la série d'une variable

$$T' = \sum (T, u w^n v) x^n$$

est à croissance polynômiale dès que  $T$  l'est, et  $R_+$ -rationnelle au cas où  $T$  l'est. De plus, soit  $S'$  la série

$$S' = \sum (S, u w^n v) x^n$$

Alors  $S'$  est rationnelle et l'on a

$$\forall n \in \mathbb{N}, \quad (S, uw^n v) / (T, uw^n v) \in \mathbb{Z}$$

Par suite la série

$$U' = \sum (U, uw^n v) x^n = \sum (S, uw^n v) / (T, uw^n v) x^n$$

est rationnelle (cela découle de Cantor (1965) si  $T$  est à croissance polynômiale et Berstel (1971) si  $T$  est  $\mathbb{R}_+$ -rationnelle). Cette dernière série vérifie donc

$$R \circ U' = 0$$

et il existe une relation de récurrence linéaire vérifiée pour tous mots  $u$  et par les séries  $\sum (U, uw^n v) x^n$ . Par suite  $U'$  est  $\mathbb{Q}$ -rationnelle, donc  $\mathbb{Z}$ -rationnelle puisque les coefficients de  $U$  sont entiers (prop. 7, § 3, chap. I).  $\square$

Remarque 1. Si  $S$  et  $T$  sont  $\mathbb{N}$ -rationnelles, leur quotient d'Hadamard, quoiqu'il soit  $\mathbb{Z}$ -rationnel, n'est pas toujours  $\mathbb{N}$ -rationnel, comme le montre un exemple de Karhumäki (1977)

Venons-en à la preuve du lemme 1.

Il nous faut quelques résultats préliminaires.

Lemme 2. Soient  $K$  un corps commutatif et  $G$  un groupe abélien libre. Soient  $A, B$ , deux parties finies non vides de  $G$ . Il existe une partie finie  $C$  de  $G$  telle que pour tous  $P, Q, R \in K[G]$  vérifiant  $P = QR$ ,  $\text{supp}(P) \subset A$  et  $\text{supp}(Q) \subset B$ ,  $Q \neq 0$ , on a  $\text{supp}(R) \subset C$ .

Preuve (i) On peut supposer que  $G$  est de type fini. Soit  $X = \{x_1, \dots, x_k\}$  une base de  $G$  et  $M$  le monoïde engendré par  $X$  :  $M$  est un monoïde abélien librement engendré par  $X$  et la sous-algèbre  $K[M]$  de  $K[G]$  s'identifie à l'algèbre des polynômes  $K[X] = K[x_1, \dots, x_k]$ . Nous dirons que le polynôme non nul  $P \in K[X]$  est *normalisé* (dans cette preuve) si les éléments de  $\text{supp}(P)$

sont sans diviseurs communs dans  $M$ , i.e. si pour tout  $i$ , il existe  $m \in \text{supp}(P)$  tel que  $m \nmid x_i$   $M$ . Pour tout  $P \in K[G]$  non nul, il existe un et un seul élément  $g$  de  $G$  tel que  $g^{-1}P$  soit dans  $K[X]$  et soit normalisé : nous posons  $g = c(P)$  et  $\bar{P} = g^{-1}P$ . On a alors  $c(PQ) = c(P)c(Q)$  et  $\overline{PQ} = \bar{P}\bar{Q}$ . En effet,  $PQ = c(P)c(Q)\bar{P}\bar{Q} = c(PQ)\bar{P}\bar{Q}$  et il suffit donc de montrer que  $\bar{P}\bar{Q}$  est normalisé ; mais si  $\bar{P}\bar{Q}$  n'est pas normalisé, il existe  $i$  tel que  $x_i$  divise  $\bar{P}\bar{Q}$ , donc  $x_i$  divise  $\bar{P}$  ou  $\bar{Q}$ , ce qui contredit le fait que  $\bar{P}$  et  $\bar{Q}$  sont normalisés.

(ii) Soient  $\bar{A}$  une partie finie de  $M$  ; il est clair qu'il existe une partie finie  $\bar{C}$  de  $M$  telle que pour tous  $P' \neq 0, R' \in K[X]$  tels que  $\text{supp}(P') \subset \bar{A}$ ,  $R'$  divise  $P'$  implique  $\text{supp}(R') \subset \bar{C}$ . En effet,  $R'$  divise  $P'$  implique  $\deg(R') \leq \deg(P')$  et il suffit de prendre pour  $\bar{C}$  l'ensemble des  $m \in M$  de degré  $\leq \sup \{ \deg(m) \mid m \in \bar{A} \}$ .

(iii) Il existe des parties finies  $A_1$  et  $B_1$  de  $G$  telles que  $\emptyset \neq \text{supp}(P) \subset A$  implique  $c(P) \in A_1$  et  $\emptyset \neq \text{supp}(Q) \subset B$  implique  $c(Q) \in B_1$ .

(iv) Soit  $\bar{A} = M \cap A_1^{-1}A$ .

Soit  $\bar{C}$  défini à partir de  $\bar{A}$  comme en (ii). Posons

$$C = A_1 B_1^{-1} \bar{C}$$

Soient  $P, Q, R$  comme dans l'énoncé. Alors  $\bar{P} = \bar{Q}\bar{R}$  et  $\text{supp}(\bar{P}) = c(P)^{-1} \cdot \text{supp}(P) \subset A_1^{-1}A$  donc  $\text{supp}(\bar{P}) \subset \bar{A}$ . Par suite  $\text{supp}(\bar{R}) \subset \bar{C}$ . Donc  $\text{supp}(R) = c(R) \text{supp}(\bar{R}) = c(P) c(Q)^{-1} \text{supp}(\bar{R}) \subset A_1 B_1^{-1} \bar{C} = C$ .  $\square$

Lemme 3. On suppose  $K$  de caractéristique nulle. Soient  $S, T, U \in K[[x]]$  des séries rationnelles régulières telles que  $S = T \otimes U$ , que le couple  $(S, T)$  soit normal et  $T \neq 0$ . Alors toute racine de  $U$  appartient au groupe engendré par les racines de  $S$  et  $T$ .

Preuve. On peut supposer que  $K$  est algébriquement clos. Soit  $G$  le groupe multiplicatif  $K \setminus 0$  et  $t$  une indéterminée. Soit  $\varphi: K[t][G] \rightarrow K[[x]]$  l'application définie dans la proposition 1 du § 9, chap. I. Soient  $A = \sum P_i(t) \lambda_i$ ,  $B = \sum Q_j(t) \mu_j$ ,  $C = \sum R_k(t) \nu_k$  les images réciproques par des séries  $S, T, U$  respectivement, avec les  $\lambda_i, \mu_j, \nu_k$  dans  $G$  et les  $P_i, Q_j, R_k$  non nuls. On a donc, dans  $K[t][G]$ , l'égalité

$$\sum P_i(t) \lambda_i = \left( \sum Q_j(t) \mu_j \right) \left( \sum R_k(t) \nu_k \right)$$

Autrement dit, pour tout  $i$  :

$$(1) \quad P_i(t) = \sum_{\mu_j \nu_k = \lambda_i} Q_j(t) R_k(t)$$

et pour tout  $\lambda \in G \setminus \{\lambda_i \mid i\}$

$$(2) \quad 0 = \sum_{\mu_j \nu_k = \lambda} Q_j(t) R_k(t)$$

Posons  $N_0 = \{ \nu_k \mid \exists i, j \text{ tels que } \mu_j \nu_k = \lambda_i \}$

Soit  $\sim$  la relation réflexive et symétrique sur  $N = \{ \nu_k \}$  définie par

$\nu \sim \nu'$  s'il existe  $\mu$  et  $\mu'$  tels que  $\nu\mu = \nu'\mu'$ . Nous notons

encore  $\sim$  la relation d'équivalence engendrée par  $\sim$ , i.e. la fermeture transitive de  $\sim$ .

Soit  $G'$  le sous-groupe de  $G$  engendré par les  $\lambda_i$  et les

Alors tout élément de  $N$  qui est équivalent modulo  $\sim$  à un élément de  $N_0$

est dans  $G'$ . En effet, si  $\nu \in N_0$ ,  $\nu \in G'$  et si  $\nu \sim \nu'$  avec  $\nu' \in N$

alors

$$\nu = \frac{\mu'}{\mu} \nu' \in G'$$

Nous montrons maintenant que tout élément de  $N$  est équivalent à un élément

$N_0$  (et le lemme sera démontré), par l'absurde : soit  $N'$  l'ensemble des  $\nu$

qui ne sont équivalent à aucun élément de  $N_0$  ; soit

$$C' = \sum_{\nu_k \in N'} P_k(t) \nu_k \in K[t][G]$$

Si  $N' \neq \emptyset$ , alors  $C' \neq 0$ . On a  $BC' = 0$

En effet, ceci est équivalent à

$$\forall \lambda \in G, \sum_{\substack{\mu_j \nu_k = \lambda \\ \nu_k \in N'}} Q_j R_k = 0$$

Or,  $\nu_k \in N'$  implique, pour tout  $j$ , que  $\mu_j \nu_k \notin \{\lambda_i\}$ . Il suffit donc de vérifier l'égalité ci-dessus pour les  $\lambda \notin \{\lambda_i\}$ . Or, si  $\nu_k \in N'$  et  $\nu_k \mu_j = \nu_{k'} \mu_{j'}$ , alors  $\nu_k \sim \nu_{k'}$ , donc  $\nu_{k'} \in N'$ . On a donc

$$\sum_{\substack{\mu_j \nu_k = \lambda \\ \nu_k \in N'}} Q_j R_k = \sum_{\mu_j \nu_k = \lambda} Q_j R_k = 0.$$

Soit  $U' = \varphi(C') \neq 0$ . Alors  $T \theta U' = 0$ . Mais ceci implique l'existence d'un entier  $N$  tel que, pour tout  $i$ ,  $0 \leq i \leq N-1$ , ou bien

$T \theta \underline{x^i(x^N)^*}$  est nul, ou bien  $U' \theta \underline{x^i(x^N)^*}$  est nul (th. 1, § 4, chap. VII).

Si pour tout  $i$ ,  $T \theta \underline{x^i(x^N)^*} \neq 0$ , alors pour tout  $i$ ,  $U' \theta \underline{x^i(x^N)^*} = 0$ , donc  $U' = 0$ . Mais cela n'est pas. Donc il existe  $i$  tel que  $T \theta \underline{x^i(x^N)^*} \neq 0$ , d'où

$$\forall n \geq 0, \sum_j Q_j (i + nN) \mu_j^i (\mu_j^N)^n = 0$$

En vertu de l'unicité du polynôme exponentiel, il existe donc deux  $\mu_j$  dont le quotient est une racine <sup>de</sup> N-ème l'unité ; or ceci, joint au fait que le groupe engendré par les  $\mu_j$  est libre implique  $N = 1$ . Mais alors  $T = 0$ , ce qui est faux. Par suite  $N'$  est vide et  $N \subset G'$ .  $\square$

Remarque 2. On a montré en fait que tout  $\nu$  s'écrit

$$\nu = \frac{\lambda_1 \mu_2 \dots \mu_r}{\mu'_1 \dots \mu'_r}$$

sous l'hypothèse, un peu plus faible, qu'aucun quotient  $\neq 1$  de deux  $\mu_j$  n'est une racine de l'unité.

Lemme 2. ( $K$  de caractéristique nulle) Soient  $P$  et  $Q$  dans  $K[x]$  dont les racines engendrent un groupe abélien libre. Il existe un polynôme  $R$  tel que : Pour toutes séries rationnelles régulières  $S, T, U$  telles que le couple  $(S, T)$  soit normal, que  $T \neq 0$ , que  $P \circ S = 0, T \circ U = 0$  et que  $S = T \circ U$ , on a  $R \circ U = 0$ .

Preuve. Soit  $G$  le groupe engendré par les racines de  $P$  et  $Q$ ,  $t$  une indéterminée,  $t^{(*)}$  le groupe libre engendré par  $t$ . Soient  $A$  et  $B$  les parties finies du groupe abélien libre  $G \times t^{(*)}$  définies par

$$A = \{ (\lambda, t^r) \mid \lambda \text{ racine de } P \text{ et } 0 \leq r < \text{multiplicité de } \lambda \}$$

$$B = \{ (\mu, t^r) \mid \mu \text{ racine de } Q \text{ et } 0 \leq r < \text{multiplicité de } \mu \}$$

Soit  $C$  la partie finie de  $G \times t^{(*)}$  donnée par le lemme 2. Soient  $p_1$  et  $p_2$  les projections  $G \times t^{(*)} \rightarrow G$  et  $G \times t^{(*)} \rightarrow t^{(*)}$ . Soient  $N = p_1(C)$  et  $s = \sup(p_2(C)) + 1$ . Soit

$$R = \prod_{\nu \in N} (x - \nu)^s \in K[x]$$

Soient  $S, T, U$  comme dans l'énoncé. Alors toute racine de  $U$  est dans  $G$  (lemme 3). Soit  $\varphi$  l'homomorphisme injectif

$$K[t][G] \rightarrow K[[x]]$$

décrit par  $\sum P_g g \mapsto \sum (\sum P_g(n) g^n) x^n$  (voir prop. 1, § 9, chap. I).

Alors il existe  $X, Y, Z$  tels que  $\varphi(X) = S, \varphi(Y) = T, \varphi(Z) = U$ . On a  $X = YZ$ . Or  $K[t][G]$  est isomorphe à  $K[t^* \times G]$  qui s'injecte dans  $K[t^{(*)} \times G]$ . Moyennant cet isomorphe, on a

$$\text{supp}(X) \subset A, \quad \text{supp}(Y) \subset B$$

Donc  $\text{supp}(Z) \subset C$ . Donc, il existe des polynômes  $R_\nu(t)$ ,  $\nu \in N$ ,  $\deg(R_\nu) < s$  tels que

$$\forall n, (U, x^n) = \sum_{v \in \Lambda} R_v(n) v^n$$

Donc  $R \circ U = 0$   $\square$

Preuve du lemme 1. (i) Posons  $P = x^p P_1$ ,  $Q = x^q Q_1$  avec  $P_1(0) \neq 0$ ,

\*0. Soit  $N-1$  l'entier ne dépendant que de  $P$  et  $Q$ , dont l'existence et les propriétés sont énoncées dans la proposition 3 du § 9, chap. I. Alors les racines des polynômes  $P_1^{(N)}$  et  $Q_1^{(N)}$  (cf. déf. 3, § 9, chap. I) engendrent un groupe libre. Soit  $R_1$  le polynôme donné par le lemme 4 (où l'on remplace  $P$  par  $P_1^{(N)}$  et  $Q$  par  $Q_1^{(N)}$ ).

Soit  $R(x) = x^{\sup(p,q)} R_2$ , avec  $R_2 = R_1(x^N)$

Soient  $S, T, U$  comme dans l'énoncé.

(i) Nous supposons d'abord  $S, T$  et  $U$  régulières. Soient  $S_0, \dots, S_{N-1}$  (resp.  $T_0, \dots, T_{N-1}$ , resp.  $U_0, \dots, U_{N-1}$ ) les séries dont l'emboîtement est égal à  $S$  (resp.  $T$ , resp.  $U$ ). Comme  $S$  et  $T$  sont régulières, on a  $P_1 \circ S = 0$ ,  $Q_1 \circ T = 0$ , donc (prop. 3, § 9, chap. I), pour tout  $k$ ,  $0 \leq k \leq N-1$

$$P_1^{(N)} \circ S_k = 0, \quad Q_1^{(N)} \circ T_k = 0.$$

De plus, le couple  $(S_k, T_k)$  est normal,  $S_k = T_k \otimes U_k$  et  $T_k = \sum b_{k+nN} x^n \neq 0$ . Donc (lemme 4), on a  $R_1 \circ U_k = 0$ . Ceci implique  $R_2 \circ U = 0$ .

(ii) Si  $S$  et  $T$  sont régulières,  $U$  l'est aussi (et l'on est ramené au cas précédent). En effet, soit  $U = \sum c_n x^n$ . Posons

$$a_n = \sum_{\lambda} \lambda^n P_{\lambda}(n), \quad b_n = \sum_{\mu} \mu^n Q_{\mu}(n) \quad (\text{pour tous } n)$$

et  $c_n = \sum_v v^n R_v(n)$  (pour tous  $n \geq 0$ ). Alors  $\forall n \geq 0$ ,

$$(\sum \lambda^n \lambda^h P_{\lambda}(n+h)) = (\sum \mu^n \mu^h Q_{\mu}(n+h)) (\sum v^n v^h R_v(n+h)) \quad \text{donc en}$$

vertu de l'unicité du polynôme exponentiel

$$\forall \lambda, \quad \lambda^h P_\lambda(t+h) = \sum_{\mu \vee \lambda} \mu^h Q_\mu(t+h) \vee^h R_\vee(t+h)$$

$$\text{d'où} \quad P_\lambda(t) = \sum_{\mu \vee \lambda} Q_\mu(t) R_\vee(t)$$

On en déduit

$$\forall n \geq 0, \quad a_n = b_n \sum \vee^n R_\vee(n) = b_n c_n$$

$$\text{donc} \quad c_n = \sum \vee^n R_\vee(n) \quad \text{pour tout} \quad n \geq 0.$$

Donc  $U$  est régulière.

(iii) Si  $S, T, U$  sont quelconques, soit  $s = \sup(p, q)$ . Alors  $x^s \circ S$

$x^s \circ T$  sont régulières et l'on a  $(x^s \circ S) = (x^s \circ T) \oplus (x^s \circ U)$ .

D'après (ii),  $x^s \circ U$  est régulière. De plus,  $P_1 \circ (x^s \circ S) = 0$  et

$Q_1 \circ (x^s \circ T) = 0$ . Par suite, d'après (i),  $R_2 \circ (x^s \circ U) = 0$ , donc

$$R \circ U = 0. \quad \square$$

## CHAPITRE V - VARIÉTÉS

-----

Le théorème d'Eilenberg affirmant qu'il y a bijection entre pseudovariétés de monoïdes finis et variétés de langages rationnels a été le point de départ de nombreuses investigations sur les rapports étroits entre ces langages et ces monoïdes. Nous définissons ici la notion de variété de séries rationnelles et établissons un analogue au théorème ci-dessus (où les monoïdes finis sont remplacés par des algèbres de dimension finie). Nous amorçons l'étude des variétés de séries rationnelles : les résultats obtenus montrent que la hiérarchie des variétés de séries est plus fine que celle des langages. Bon nombre de variétés définies par des restrictions naturelles sur les séries s'avèrent correspondre à des variétés d'algèbres ayant des propriétés algébriques classiques : ainsi une variété est non littérale si et seulement si la variété d'algèbres associée est composée d'algèbres semi-simples. Plus précisément, nous caractérisons les variétés littérales, et aussi la plus grande variété (propre) non littérale (th. 1, § 3). Nous donnons plusieurs caractérisations

des variétés fermées par produit (th. 1 et 3, § 4), en particulier de la plus petite variété non nulle fermée par produit (prop. 2) : elle s'apparente à la variété des langages rationnels apériodiques ("star-free") et nous obtenons ainsi le théorème analogue à celui de Schützenberger sur les monoïdes apériodiques (th. 2, § 4) ; nous caractérisons les variétés fermées par produit de Hadamard et la plus grande parmi ces variétés (th. 1, § 5) ; enfin, nous définissons les variétés équationnelles et ultimement équationnelles, et montrons que si le corps des scalaires est fini, toute variété est ultimement équationnelle (th. 1, § 6), mais qu'il n'en est plus ainsi lorsqu'il est infini.

Dans ce chapitre,  $K$  désigne un *corps commutatif*. Les conventions sur les algèbres, telles qu'elles sont exposées au début du chapitre II, sont maintenues ici. Les alphabets sont supposés *finis*. On considérera souvent les séries formelles comme des formes linéaires sur l'espace des polynômes (cf. § 2, chap. I).

# 1. LE THEOREME DES VARIETES

Définition 1. Une *pseudo-variété* d'algèbres est une classe non vide  $V$  d'algèbres qui vérifie :

- Si  $\pi \in V$  et  $\pi \rightarrow \pi'$  est surjectif, alors  $\pi' \in V$ .
- Si  $\pi \in V$  et  $\pi' \rightarrow \pi$  est injectif, alors  $\pi' \in V$ .
- Si  $\pi, \pi' \in V$ , alors  $\pi \times \pi' \in V$ .

Remarque 1. Rappelons que  $\pi' < \pi$  signifie que  $\pi'$  est isomorphe à un quotient d'une sous-algèbre de  $\pi$ . Les deux premières conditions de la définition 1 peuvent donc être remplacées par l'unique condition

- Si  $\pi \in V$  et  $\pi' < \pi$ , alors  $\pi' \in V$ .

Définition 2. Une  $\alpha$ -variété est une pseudo-variété d'algèbres de dimension finie.

Soit  $X$  un alphabet,  $u$  et  $v$  des mots sur  $X$  et  $S \in K\langle\langle X \rangle\rangle$ . Rappelons les notations suivantes :

$$u \circ S \circ v = v^{-1} S u^{-1} = \sum_{w \in X^*} (S, v w u) w$$

(cf. chap. I, § 3).

Pour simplifier le vocabulaire, nous allons faire l'hypothèse que tous les alphabets considérés sont des sous-ensembles finis d'un ensemble dénombrable fixé. On pourra ainsi parler de *l'ensemble de tous les alphabets*, de *l'ensemble des séries formelles* sur ces alphabets, etc... De la même manière, nous pouvons parler de *l'ensemble des algèbres de type fini*, étant entendu qu'une telle algèbre sera considérée comme quotient d'une algèbre  $K\langle X \rangle$ , où  $X$  est un alphabet.

Définition 3. Une *s-variété*  $\mathcal{V}$  est une application de l'ensemble des alphabets dans l'ensemble des séries rationnelles, notée  $X \mapsto X^* \mathcal{V}$ , telle que

- $X^* \mathcal{V}$  est un sous-espace vectoriel de  $K\langle\langle X \rangle\rangle$ .
- Si  $S \in X^* \mathcal{V}$  et  $u, v \in X^*$  alors  $u \circ S \circ v \in X^* \mathcal{V}$ .
- Si  $Y$  est un autre alphabet et  $\mu : K\langle Y \rangle \rightarrow K\langle X \rangle$  un morphisme d'algèbres, alors  $S \in X^* \mathcal{V}$  implique  $S \circ \mu \in Y^* \mathcal{V}$ .

Remarque 2. Nous utiliserons souvent l'abus de notation suivant : si  $S \in X^* \mathcal{V}$  nous écrirons  $S \in \mathcal{V}$ .

S. Eilenberg (1976, chap. VII, § 3) a établi qu'il y a bijection entre pseudovariétés de monoïdes finis et variétés de langages. Nous obtenons le résultat analogue pour *a-variétés* et *s-variétés*.

Théorème 1. Soit  $\mathcal{V}$  une *s-variété* et  $\mathcal{V}$  la *a-variété* engendrée par les algèbres syntactiques des séries dans  $\mathcal{V}$  (nous notons ceci  $\mathcal{V} \mapsto \mathcal{V}$ ).

L'application ainsi définie est une bijection entre *s-variétés* et *a-variétés* et l'application réciproque  $\mathcal{V} \mapsto \mathcal{V}$  est définie par :  $\mathcal{V}$  est l'ensemble des séries formelles dont l'algèbre syntactique est dans  $\mathcal{V}$ .

Nous avons besoin d'un certain nombre de résultats préliminaires.

Lemme 1. Soit  $\mathcal{M}$  une algèbre de dimension finie. Il existe des algèbres  $\mathcal{M}_1, \dots, \mathcal{M}_n$  quotients de  $\mathcal{M}$ , qui sont syntactiques et telles que l'homomorphisme canonique  $\mathcal{M} \rightarrow \prod \mathcal{M}_i$  soit injectif.

Preuve. Soit  $X$  un alphabet tel qu'il existe une surjection  $\nu : K\langle X \rangle \rightarrow \mathcal{M}$ . Soit  $\varphi_1, \dots, \varphi_n$  une base du dual de  $\mathcal{M}$  et  $V_i, S_i$  la série reconnaissant  $\varphi_i \circ \nu$ . Soit  $\mathcal{M}_i$  l'algèbre syntactique de  $S_i$ . Il existe un homomorphisme surjectif  $\mu_i : \mathcal{M} \rightarrow \mathcal{M}_i$  tel que  $\mu_i \circ \nu = \mu_{S_i}$ .

Soit  $\mu : \mathbb{M} \rightarrow \prod \mathbb{M}_i$  le produit des  $\mu_i$ . Si  $m \in \mathbb{M}$ , il existe  $P \in K\langle X \rangle$  tel que  $v(P) = m$  et :  $\mu(m) = 0 \Rightarrow \forall i, \mu_i(m) = 0 \Rightarrow \forall i, \mu_{S_i}(P) = 0 \Rightarrow \forall i, (S_i, P) = 0$  (puisque  $S_i = \varphi_{S_i} \circ \mu_{S_i}$ )  
 $\Rightarrow \forall i, \varphi_i(m) = 0$  (puisque  $\varphi_i(m) = \varphi_i \circ v(P) = (S_i, P)$ )  
 $\Rightarrow m = 0$ .  $\square$

Nous en déduisons le

Lemme 2. Une a-variété est engendrée par les algèbres syntactiques qu'elle contient.

Preuve. Soit  $V$  une a-variété et  $V'$  la a-variété engendrée par les algèbres syntactiques appartenant à  $V$ . On a clairement  $V' \subset V$ . Soit  $\mathbb{M} \in V$ . D'après le lemme 1, il existe des algèbres  $\mathbb{M}_1, \dots, \mathbb{M}_n$ , quotients de  $\mathbb{M}$ , donc appartenant à  $V$ , qui sont syntactiques, donc appartiennent à  $V'$ , et telles que

$$\mathbb{M} \rightarrow \prod \mathbb{M}_i$$

soit injectif. Alors  $\mathbb{M}_i \in V'$  implique  $\prod \mathbb{M}_i \in V'$  donc  $\mathbb{M} \in V'$ .  $\square$

Lemme 3. Soit  $V$  une s-variété et  $S \in X^*V$ . Soit  $\varphi$  une forme linéaire sur  $\mathbb{M}_S$ . Alors  $\varphi \circ \mu_S \in X^*V$ .

Preuve. D'après la prop. 1 du § 1, chap. III,  $\varphi \circ \mu_S$  est combinaison linéaire des séries  $u \circ S \circ v$  ( $u, v \in X^*$ ). Par suite,  $\varphi \circ \mu_S \in X^*V$ .  $\square$

Lemme 4. Soient  $S_1$  et  $S_2 \in K\langle\langle X \rangle\rangle$ , reconnues par les algèbres  $\mathbb{M}_1$  et  $\mathbb{M}_2$  respectivement, et  $\lambda_1, \lambda_2 \in K$ . Alors  $\mathbb{M}_1 \times \mathbb{M}_2$  reconnaît  $\lambda_1 S_1 + \lambda_2 S_2$ .

Preuve. Soit  $\mu : K\langle X \rangle \rightarrow \mathbb{M}_1 \times \mathbb{M}_2$   
 $P \mapsto (\mu_1(P), \mu_2(P))$

et

$$\varphi: \mathbb{M}_1 \times \mathbb{M}_2 \rightarrow K$$

$$\varphi(m_1, m_2) = \lambda_1 \varphi_1(m_1) + \lambda_2 \varphi_2(m_2)$$

Alors

$$\forall w \in X^*$$

$$\begin{aligned} \varphi \circ \mu(w) &= \lambda_1 \varphi_1 \circ \mu_1(w) + \lambda_2 \varphi_2 \circ \mu_2(w) \\ &= \lambda_1 (S_1, w) + \lambda_2 (S_2, w) \end{aligned}$$

Par suite  $\mathbb{M}_1 \times \mathbb{M}_2$  reconnaît  $\lambda_1 S_1 + \lambda_2 S_2$ .  $\square$

Lemme 5. Soit  $S \in K\langle\langle X \rangle\rangle$  reconnue par  $\mathbb{M}$ ,  $u, v \in X^*$  et  $\nu$  un morphisme d'algèbres  $K\langle Y \rangle \rightarrow K\langle X \rangle$  où  $Y$  est un autre alphabet. Alors  $\mathbb{M}$  reconnaît  $u \circ S \circ v$  et  $S \circ \nu$ .

Preuve. On a

$$S \circ \nu(w) = \varphi \circ (\mu \circ \nu)(w)$$

donc  $\mathbb{M}$  reconnaît  $S \circ \nu$ . Soit  $\psi$  la forme linéaire sur  $\mathbb{M}$  définie par

$$\psi(m) = \varphi(\mu(v) m \mu(u))$$

Alors pour tout mot  $w$

$$\psi \circ \mu(w) = \varphi \circ \mu(vwu) = (S, vwu) = (u \circ S \circ v, w)$$

donc  $\mathbb{M}$  reconnaît  $u \circ S \circ v$ .  $\square$

Lemme 6. Soit  $V$  une  $\alpha$ -variété engendrée par une famille d'algèbres  $\mathcal{F}$ . Alors  $\mathbb{M} \in V$  si et seulement s'il existe des algèbres  $\mathbb{M}_1, \dots, \mathbb{M}_n \in \mathcal{F}$  telles que

$$\mathbb{M} < \mathbb{M}_1 \times \dots \times \mathbb{M}_n$$

Preuve. Soit  $V'$  l'ensemble des algèbres défini par :

$\mathbb{M} \in V'$  si et seulement s'il existe des algèbres  $\mathbb{M}_1, \dots, \mathbb{M}_n$  telles que  $\mathbb{M} < \mathbb{M}_1 \times \dots \times \mathbb{M}_n$ .

Si  $\pi\bar{b}' < \pi\bar{b}$  et  $\pi\bar{b} \in V'$ , on a  $\pi\bar{b}' \in V'$  car  $<$  est une relation transitive. De plus si  $\pi\bar{b}, \pi\bar{b}' \in V'$  alors  $\pi\bar{b} \times \pi\bar{b}' \in V'$  car  $\pi\bar{b} < \pi\bar{b}'$ ,  $\pi\bar{b}' < \pi\bar{b}$  implique  $\pi\bar{b} \times \pi\bar{b}' < \pi\bar{b} \times \pi\bar{b}'$ . Ceci prouve que  $V'$  est une a-variété. Comme  $\mathcal{F} \subset V'$ , on a  $V \subset V'$ . Réciproquement on a  $\mathcal{F} \subset V$  donc tout produit fini d'algèbres de  $\mathcal{F}$  appartient à  $V$ , ainsi que toute algèbre divisant un tel produit, puisque  $V$  est une variété. Par suite  $V' \subset V$ .

Lemme 6. Soit  $V$  une a-variété et  $S$  une série formelle. On a  $\pi\bar{b}_S \in V$  si et seulement s'il existe  $\pi\bar{b} \in V$  telle que  $\pi\bar{b}$  reconnaisse  $S$ .

Preuve. La condition est nécessaire puisque  $\pi\bar{b}_S$  reconnaît  $S$ . Réciproquement s'il existe  $\pi\bar{b} \in V$  reconnaissant  $S$  alors  $\pi\bar{b}_S$  divise  $\pi\bar{b}$  (corollaire au th. 1, § 1, chap. II) donc  $\pi\bar{b}_S \in V$ .  $\square$

Preuve du théorème 1. (inspirée de Eilenberg, 1976, chap. VII). Si  $V$  est une a-variété et  $V \twoheadrightarrow \mathcal{U}$  alors  $\mathcal{U}$  est une s-variété, d'après les lemmes 4, 5 et 6. De même si  $\mathcal{U}$  est une s-variété et  $\mathcal{U} \twoheadrightarrow V$ , alors  $V$  est une a-variété.

1. Soit  $V$  une a-variété et  $V \twoheadrightarrow \mathcal{U} \twoheadrightarrow V'$ .  $V'$  est engendré par les  $\pi\bar{b}_S$  ( $S \in \mathcal{U}$ ), par définition. Or,  $S \in \mathcal{U} \Rightarrow \pi\bar{b}_S \in V$ , donc  $V' \subset V$ . De plus  $V$  est engendré par les  $\pi\bar{b}_S$  tels que  $\pi\bar{b}_S \in V$  (lemme 2). Or,  $\pi\bar{b}_S \in V \Rightarrow S \in \mathcal{U} \Rightarrow \pi\bar{b}_S \in V'$  donc  $V \subset V'$ .
2. Soit  $\mathcal{U}$  une s-variété et  $\mathcal{U} \twoheadrightarrow V \twoheadrightarrow V'$ . Si  $S \in \mathcal{U}$  alors  $\pi\bar{b}_S \in V$  donc  $S \in V'$ . Par suite  $\mathcal{U} \subset V'$ . Pour la réciproque, considérons  $S \in X^* \mathcal{U}'$ . On a  $\pi\bar{b}_S \in V$ . Or  $V$  est engendré par les  $\pi\bar{b}_T$  telles que  $T \in \mathcal{U}$  donc il existe  $T_1, \dots, T_n \in \mathcal{U}$  tels que  $\pi\bar{b}_S < \pi\bar{b}_{T_1} \dots \pi\bar{b}_{T_n}$  (lemme 6).

Soit  $X_i$  l'alphabet de  $T_i$ . Nous posons

$$\pi\bar{b}_i = \pi\bar{b}_{T_i}, \quad \mu_i = \mu_{T_i}, \quad \varphi_i = \varphi_{T_i}$$

On a par définition :  $T_i = \varphi_i \circ \mu_i$ .

Soit  $W = \prod K \langle X_i \rangle$ ,  $\pi_6 = \prod \pi_{6_i}$  et

$$\mu: W \rightarrow \pi_6$$

$$(P_1, \dots, P_n) \mapsto (\mu_1(P_1), \dots, \mu_n(P_n))$$

Comme chaque  $\mu_i$  est surjectif,  $\mu$  est surjectif. Comme  $\pi_{6_S} < \pi_6$ , il existe une sous-algèbre  $\pi_{6'}$  de  $\pi_6$  et un morphisme surjectif.

$$\beta: \pi_{6'} \rightarrow \pi_{6_S}$$

Comme  $K \langle X \rangle$  est libre et  $\beta$  surjectif, il existe un morphisme  $\alpha$  tel qu'on ait le diagramme

$$\begin{array}{ccc} \pi_{6'} & \xrightarrow{\beta} & \pi_{6_S} \\ \alpha \swarrow & & \nearrow \mu_S \\ & K \langle X \rangle & \end{array}$$

Soit  $\psi$  la forme linéaire sur  $\pi_{6'}$

$$\psi = \varphi_S \circ \beta$$

et  $\bar{\psi}$  un prolongement quelconque de  $\psi$  à  $\pi_6$ . Alors  $\forall P \in K \langle X \rangle$   $\alpha(P) \in \pi_{6'}$ , donc  $\bar{\psi} \circ \alpha(P) = \psi \circ \alpha(P) = \varphi_S \circ \beta \circ \alpha(P) = \varphi_S \circ \mu_S(P) = (S, P)$ . De plus,  $\mu$  étant surjectif et  $K \langle X \rangle$  libre, il existe un morphisme  $\gamma$  tel qu'on ait le diagramme

$$\begin{array}{ccc} & \pi_6 & \\ \mu \nearrow & & \nwarrow \alpha \\ W & \xleftarrow{\gamma} & K \langle X \rangle \end{array}$$

Posons  $\gamma = (\gamma_1, \dots, \gamma_n)$  où  $\gamma_i: K \langle X \rangle \rightarrow K \langle X_i \rangle$

$$\alpha(P) = (\alpha_1(P), \dots, \alpha_n(P)) \text{ où } \alpha_i: K \langle X \rangle \rightarrow \pi_{6_i}$$

$$\bar{\psi} = \sum \psi_i \quad \text{où } \psi_i: \pi_{6_i} \rightarrow K$$

Alors  $\alpha = \mu \circ \gamma \Rightarrow \alpha_i = \mu_i \circ \gamma_i$ .

Alors

$$(S, P) = \bar{\psi} \circ \alpha(P) = \sum \psi_i \circ \alpha_i(P) = \sum \psi_i \circ \mu_i \circ \gamma_i(P)$$

Soit  $S_i \in K \langle\langle X \rangle\rangle$ ,  $S_i = \psi_i \circ \mu_i \circ \gamma_i$ . Alors

$$S = \sum S_i$$

Or  $\psi_i \circ \mu_i \in X^* \mathcal{V}$  (lemme 3) donc  $S_i = \psi_i \circ \mu_i \circ \gamma_i \in X^* \mathcal{V}$ .

D'où  $S \in X^* \mathcal{V}$  et  $\mathcal{V}^* \subset \mathcal{V}$ .  $\square$

Le lemme suivant nous sera utile dans la suite.

Lemme 7. Soit  $\mathcal{V}$  une a-variété et  $\mathcal{U}$  une s-variété telles que  $\mathcal{V} \leftrightarrow \mathcal{U}$ .

Soit  $\mathcal{M}$  une algèbre. Alors  $\mathcal{M} \in \mathcal{V}$  si et seulement si toute série reconnue par  $\mathcal{M}$  est dans  $\mathcal{U}$ .

Preuve. La condition est clairement nécessaire. Réciproquement, soit  $\mathcal{M}$  telle que toute série reconnue par  $\mathcal{M}$  soit dans  $\mathcal{U}$ . Il existe des séries  $S_1, \dots, S_n$  telles que les  $\mathcal{M}_{S_i}$  soient quotient de  $\mathcal{M}$  et que  $\mathcal{M} < \prod \mathcal{M}_{S_i}$  (lemme 1). Alors  $\mathcal{M}$  reconnaît les  $S_i$ , donc  $S_i \in \mathcal{U}$ . Par suite,  $\mathcal{M}_{S_i} \in \mathcal{V}$  et  $\mathcal{M} \in \mathcal{V}$ .

## 2. QUELQUES VARIÉTÉS PARTICULIÈRES

Dans la suite  $\mathcal{V}$  désignera une a-variété et  $\mathcal{U}$  la s-variété correspondante.

### a. Plus petites variétés

La a-variété nulle  $\mathcal{V}$  est réduite à l'algèbre nulle ;  $\mathcal{U}$  est alors définie par : pour tout alphabet  $X$ ,  $X^* \mathcal{U} = 0$ .

La plus petite  $a$ -variété non nulle  $V$  est clairement la  $a$ -variété engendrée par l'algèbre  $K$ . Elle contient donc toutes les algèbres  $K^n$  ( $n \geq 0$ ) ; or on montre aisément que toute sous-algèbre et tout quotient de  $K^n$  est de la forme  $K^m$  ( $0 \leq m \leq n$ ). Par suite

$$V = \{ K^n \mid n \geq 0 \}$$

Définition 1. Nous appellerons *série géométrique* une série dont l'algèbre syntactique est isomorphe à  $K$ .

Lemme 1. Soit  $S \in K \langle\langle X \rangle\rangle$ . Alors  $S$  est une série géométrique si et seulement s'il existe des scalaires  $a_x$  ( $x \in X$ ), non tous nuls, et  $b \neq 0$  tels que  $\forall w \in X^* \quad (S, w) = b \prod_{x \in X} a_x^{|w|_x}$

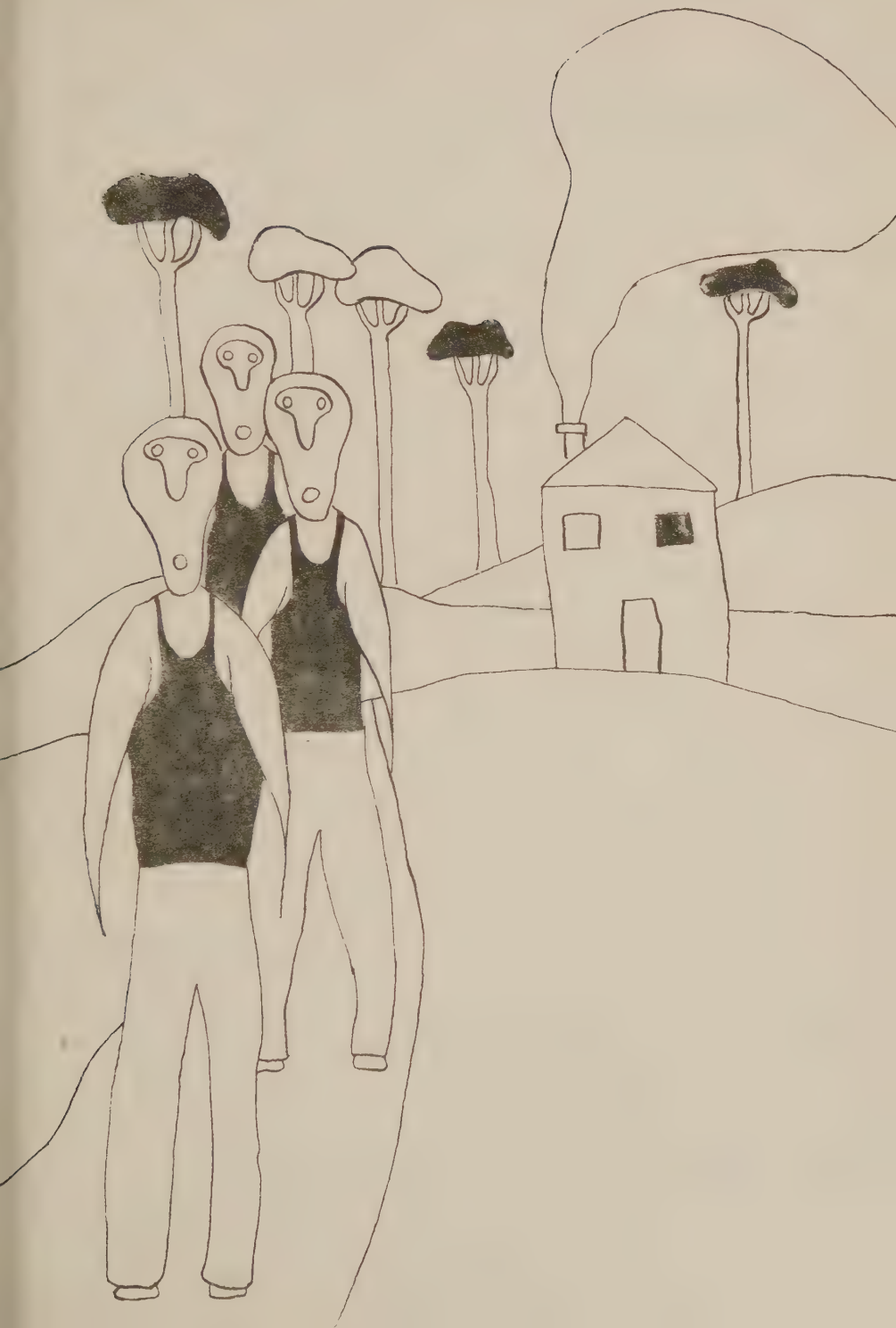
Dans ce cas  $S = b (1 - \sum_{x \in X} a_x x)^{-1} = b (\sum a_x x)^*$

Preuve. Soit  $S$  une série géométrique et  $a_x = \mu_S(x)$  ( $x \in X$ ),  $b = \varphi_S(1)$ . Si  $w \in X^*$ , on a  $\mu_S(w) = \prod_{x \in X} a_x^{|w|_x}$  et  $(S, w) = b \mu_S(w)$ . Les  $a_x$  ne sont pas tous nuls et  $B$  est non nul, sinon  $S = 0$  et  $\mathcal{H}_S = 0$ . Réciproquement si  $S$  est comme ci-dessus, soit  $\mu : K \langle\langle X \rangle\rangle \rightarrow K$  le morphisme défini par  $\mu(x) = a_x$  et  $\varphi : K \rightarrow K$ ,  $\varphi(k) = bk$ . Alors  $(S, w) = \varphi \circ \mu(w)$ , donc  $K$  reconnaît  $S$ . Si  $K$  n'était pas isomorphe à l'algèbre syntactique de  $S$ , on aurait  $\mathcal{H}_S = 0$  et  $S = 0$ , ce qui contredit les hypothèses. Par suite  $\mathcal{H}_S = K$  et  $S$  est géométrique.

Un calcul simple montre que

$$(\sum_x a_x x)^* = (1 - \sum_x a_x x)^{-1} = \sum_{w \in X^*} w \prod_x a_x^{|w|_x} \quad \square$$

Lemme 2. Soient  $\mathcal{H}_1, \mathcal{H}_2, \dots, \mathcal{H}_n$  des algèbres et  $S$  une série reconnue par  $\mathcal{H}_1 \times \mathcal{H}_2 \times \dots \times \mathcal{H}_n$ . Il existe des séries  $S_i$  reconnues par  $\mathcal{H}_i$  ( $i = 1, \dots, n$ ) telles que  $S = S_1 + S_2 + \dots + S_n$ .





Preuve. Soit  $\mu : X^* \rightarrow \prod \mathbb{H}_i$ ,  $\varphi : \prod \mathbb{H}_i \rightarrow K$  tels que  $S = \varphi \circ \mu$ .

Soient  $\mu_i$  la projection de  $\mu$  sur  $\mathbb{H}_i$  et  $\varphi_i$  la restriction de  $\varphi$  à  $\mathbb{H}_i$ . Alors

$$S = \varphi \circ \mu = \sum \varphi_i \circ \mu_i$$

et le lemme en découle.  $\square$

Revenons à la  $a$ -variété  $V$  ci-dessus. Soit  $\mathcal{V}$  la  $s$ -variété correspondante.

Si  $S \in X^* \mathcal{V}$ , d'après le lemme 2,  $S$  est somme de séries géométriques.  $\square$

#### b. Plus grande variété

L'ensemble (!) de toutes les algèbres de dimension finie est la plus grande  $a$ -variété : nous la noterons  $Alg$ . La  $s$ -variété correspondante est constituée de toutes les séries rationnelles : nous la notons  $Rat$ .

Lemme 3. Soit  $V$  une  $a$ -variété contenant  $K^n \times^n$  pour tout  $n \gg 1$ . Alors  $V = Alg$ .

Preuve. Ceci vient de ce que toute algèbre de dimension finie s'injecte dans une algèbre de matrices.  $\square$

#### c. Variétés commutatives.

Une  $a$ -variété est dite *commutative* si toutes les algèbres qu'elle contient sont commutatives ; il est équivalent de dire que la  $s$ -variété correspondante est formée de séries échangeables (cf. définition 2, § 3, chap. III).

En particulier l'ensemble de toutes les algèbres commutatives de dimension finie est une  $a$ -variété et l'ensemble de toutes les séries rationnelles échangeables une  $s$ -variété.

### 3. VARIETES LITTERALES

Nous posons la définition suivante (cf. Perrot, 1978).

Définition 1. Une  $s$ -variété  $\mathcal{V}$  est *littérale* s'il existe un alphabet  $X$ , une lettre  $x \in X$  tels que  $x \in X^* \mathcal{V}$ .

Lemme 1.  $\mathcal{V}$  est littérale si et seulement si  $\mathcal{V}$  contient une algèbre  $\mathbb{H}$  contenant  $\omega$  : élément nilpotent non nul.

Preuve. Si  $m \in \mathbb{H} \in \mathcal{V}$  est nilpotent non nul, on peut se ramener à  $m \neq m^2 = 0$ . Il existe une forme linéaire  $\varphi$  sur  $\mathbb{H}$  telle que  $\varphi(m) = 1$ . Soit  $X$  un alphabet,  $x \in X$  et  $\mu : K\langle X \rangle \rightarrow \mathbb{H}$  défini par  $\mu(x) = m$  et  $\mu(X \setminus x) = 0$ . Alors  $(\mathbb{H}, \mu, \varphi)$  est une représentation de la série  $x$  donc  $\mathbb{H}$  reconnaît  $x$  et  $x \in X^* \mathcal{V}$ .

Pour la réciproque, on remarque que l'algèbre syntactique  $\mathbb{H}_x$  de la série  $S = x$  contient un élément non nul de carré nul, à savoir  $\mu_x(x)$  car :

$$1 = (S, x) = \varphi_x \circ \mu_x(x) \Rightarrow \mu_x(x) \neq 0$$

et  $\forall u, v \in X^*$ ,  $(S, ux^2v) = 0$  donc  $x^2 \in \mathcal{J}_x$  et  $\mu_x(x^2) = 0$ .  $\square$

Corollaire. Si  $\mathcal{V}$  est littérale, alors pour tout alphabet  $X$  et tout  $x \in X$ , on a  $x \in X^* \mathcal{V}$ .

Théorème 1. Parmi les  $s$ -variétés non littérales, il en existe une plus grande soit  $\tilde{\mathcal{V}}$ .  $\mathcal{V}$  est alors constituée des algèbres de dimension finie qui sont produites de surcorps de  $K$ .  $\mathcal{V}$  est aussi la plus grande  $a$ -variété dont toutes les algèbres sont semi-simples.

Nous avons besoin de deux lemmes.

Lemme 2. Soit  $\mathbb{M}$  une algèbre de dimension finie. Les conditions suivantes sont équivalentes :

- (i)  $\mathbb{M}$  est sans éléments nilpotents.
- (ii)  $\mathbb{M}$  est isomorphe à un produit de surcorps de  $K$ .

Preuve. Si  $\mathbb{M}$  est sans éléments nilpotents,  $\mathbb{M}$  est sans idéaux nilpotents, donc isomorphe à un produit fini d'algèbres de la forme  $\mathcal{M}_n(D)$ , où  $D$  est un surcorps de  $K$  (Herstein, 1968, th. 2.1.8.). Mais comme  $\mathbb{M}$  est sans éléments nilpotents,  $n = 1$ , donc  $\mathbb{M}$  est isomorphe à un produit de surcorps de  $K$ . La réciproque est claire.  $\square$

Lemme 3. Soit  $\mathbb{M} = \prod_1 \mathbb{D}_i$  un produit fini de surcorps de  $K$ . Si  $\mathbb{M}' < \mathbb{M}$ ,  $\mathbb{M}$  est sans éléments nilpotents.

Preuve. C'est clair, si  $\mathbb{M}' \subset \mathbb{M}$ . On est donc ramené à  $\mathbb{M}' = \mathbb{M}/I$  où  $I$  est un idéal de  $\mathbb{M}$  (à l'aide du lemme 2). Soit  $m \in \mathbb{M}$  et  $r \geq 1$  tel que  $m^r \in I$ ;  $m$  s'écrit

$$m = \sum_i d_i$$

où  $d_i \in D_i$ . Alors

$$m^r = \sum d_i^r \in I$$

Comme  $I$  est un idéal et  $D_i$  un corps on a  $d_i \neq 0 \Rightarrow D_i \subset I$ . Donc

$$m = \sum_{i, d_i \neq 0} d_i \in I \quad \text{car} \quad \mathbb{M}'$$

est sans éléments nilpotents.  $\square$

Preuve du théorème 1. Soit  $V$  l'ensemble des algèbres de dimension finie qui sont produits de surcorps de  $K$ . D'après les lemmes 2 et 3,  $V$  est une  $a$ -variété et  $\mathbb{M} \in V \Leftrightarrow \mathbb{M}$  est sans éléments nilpotents.

Par suite, la  $s$ -variété  $\mathcal{V}$  associée à  $V$  est non littérale (lemme 1). Soit  $\mathcal{V}'$  une  $s$ -variété non littérale et  $V'$  la  $a$ -variété associée à  $\mathcal{V}'$ . Alors  $\mathcal{M} \in V' \Rightarrow \mathcal{M}$  est sans éléments nilpotents (lemme 1). Par suite  $\mathcal{M} \in \mathcal{V}'$  où  $V' \subset V$  et  $\mathcal{V}' \subset \mathcal{V}$ . Soit  $V''$  une  $a$ -variété dont toutes les algèbres sont semi-simples. Alors toute algèbre dans  $V''$  est isomorphe à un produit d'algèbres de la forme  $\mathcal{M}_n(D)$ , où  $D$  est un surcorps de  $K$  (Herstein 68, th. 2.1.8) ; mais alors  $V''$  contient  $\mathcal{M}_n(D)$  donc  $n = 1$  sinon  $V''$  contiendrait l'algèbre des matrices triangulaires d'ordre  $n$  sur  $K$ , qui n'est pas semi-simple. Par suite  $V'' \subset V$ . Par ailleurs, toute algèbre dans  $V$  est clairement semi-simple.  $\square$

Corollaire. Soit  $V$  une  $a$ -variété et  $\mathcal{V}$  la  $s$ -variété correspondante.  $\mathcal{V}$  non littérale si et seulement si toute algèbre dans  $V$  est semi-simple.

#### 4. VARIETES FERMEES PAR PRODUIT.

La définition suivante est inspirée de Perrot (1978).

Définition 1. Une  $s$ -variété  $\mathcal{V}$  est fermée par produit (sous-entendu : de Cauchy) si pour tout alphabet  $X$ , tous  $S, T \in X^* \mathcal{V}$  on a  $ST \in X^* \mathcal{V}$ .

Le résultat suivant est analogue à un résultat de Perrot pour les langages.

Proposition 1. Si  $\mathcal{V}$  est non nulle et fermée par produit,  $\mathcal{V}$  est littérale.

Preuve.  $\mathcal{V}$  est non nulle, donc  $\mathcal{V}$  contient les séries géométriques (voir 2a). Soit  $X = \{x, y\}$  : alors  $x^*, y^* \in X^* \mathcal{V}$  donc  $S = x^* y^* \in X^* \mathcal{V}$ . Or  $xy \notin \mathcal{V}_S$  et  $xyxy \in \mathcal{V}_S$  comme on le vérifie aisément. Donc  $\mathcal{M}_S$  contient un élément nilpotent et  $\mathcal{V}$  est littérale (lemme 1, § 3).  $\square$

Au produit de deux langages correspond dans la théorie des variétés de langage le produit de Schützenberger des monoïdes (voir Eilenberg, 1976, chap. IX,

Nous allons définir un produit d'algèbres qui possède des propriétés analogues.

Soient  $\mathcal{A}_1$  et  $\mathcal{A}_2$  deux algèbres. L'espace vectoriel

$$V = \mathcal{A}_1 \otimes_K \mathcal{A}_2$$

est muni canoniquement d'une structure de  $\mathcal{A}_1$ -module à gauche et de  $\mathcal{A}_2$ -module à droite et les deux opérations externes commutent.

Sur l'espace vectoriel  $\mathcal{A}_1 \times V \times \mathcal{A}_2$  nous définissons un produit de la manière suivante :

$$(1) \quad (m_1, v, m_2) (m'_1, v', m'_2) = (m_1 m'_1, m_1 v' + v m'_2, m_2 m'_2)$$

Ceci est formellement repéré par le produit matriciel

$$\begin{pmatrix} m_1 & v \\ 0 & m_2 \end{pmatrix} \begin{pmatrix} m'_1 & v' \\ 0 & m'_2 \end{pmatrix} = \begin{pmatrix} m_1 m'_1 & m_1 v' + v m'_2 \\ 0 & m_2 m'_2 \end{pmatrix}$$

On vérifie que le produit défini ci-dessus fait de  $\mathcal{A}_1 \times V \times \mathcal{A}_2$  une algèbre, dont l'élément neutre est  $(1, 0, 1)$ .

Définition 2. Le produit de Schützenberger des algèbres  $\mathcal{A}_1$  et  $\mathcal{A}_2$ , noté  $\mathcal{A}_1 \diamond \mathcal{A}_2$ , est l'algèbre  $\mathcal{A}_1 \times V \times \mathcal{A}_2$  où le produit est défini par (1).

Remarque 1. Il est facile de voir que  $\mathcal{A}_1 \times \mathcal{A}_2$  s'identifie à la fois à une sous-algèbre et à un quotient de  $\mathcal{A}_1 \diamond \mathcal{A}_2$ .

L'intérêt de ce produit est qu'il permet la reconnaissance des produits de séries.

Lemme 1. Soit  $S_i \in K\langle\langle X \rangle\rangle$  reconnues respectivement par  $\mathcal{A}_i$ ,  $i = 1, 2$ . Alors  $\mathcal{A}_1 \diamond \mathcal{A}_2$  reconnaît  $S_1 S_2$ .

Preuve. Soit  $(\pi_i, \mu_i, \varphi_i)$  une représentation de  $S_i$ ,  $i = 1, 2$ . Soit  $\pi = \pi_1 \otimes \pi_2$  et

$$\mu: X^* \rightarrow \pi$$

$$w \mapsto (\mu_1 w, \nu w, \mu_2 w)$$

où  $\nu$  est définie par

$$\nu w = \sum_{\substack{w = uv \\ u \neq 1}} \mu_1 u \otimes \mu_2 v$$

On a :

$$\begin{aligned} \nu(w w') &= \sum_{\substack{w w' = uv \\ u \neq 1}} \mu_1 u \otimes \mu_2 v = \sum_{\substack{w = uv \\ u \neq 1}} \mu_1 u \otimes \mu_2 v w' + \sum_{\substack{w' = uv \\ u \neq 1}} \mu_1 w u \otimes \mu_2 v \\ &= \left( \sum_{\substack{w = uv \\ u \neq 1}} \mu_1 u \otimes \mu_2 v \right) \mu_2 w' + \mu_1 w \left( \sum_{\substack{w' = uv \\ u \neq 1}} \mu_1 u \otimes \mu_2 v \right) \\ &= \nu w \cdot \mu_2 w' + \mu_1 w \cdot \nu w' \end{aligned}$$

Par suite :

$$\begin{aligned} \mu(w w') &= (\mu_1 w w', \mu_1 w \cdot \nu w' + \nu w \cdot \mu_2 w', \mu_2 w w') \\ &= (\mu_1 w, \nu w, \mu_2 w) (\mu_1 w', \nu w', \mu_2 w') = \mu w \cdot \mu w'. \end{aligned}$$

Par suite  $\mu$  se prolonge en un homomorphisme d'algèbres  $K\langle X \rangle \rightarrow \pi$ .

Soit  $\varphi$  la forme linéaire sur  $\pi$  définie par  $\varphi(m_1, m'_1 \otimes m'_2, m_2) = \varphi_1(m'_1) \varphi_2(m'_2)$ .

On a alors :

$$\varphi \circ \mu w = \sum_{\substack{w = uv \\ u \neq 1}} \varphi_1(\mu_1 u) \cdot \varphi_2(\mu_2 v) = \sum_{\substack{w = uv \\ u \neq 1}} (S_1, u) (S_2, v)$$

Donc  $\varphi \circ \mu$  est égal à la série  $S'_1 S_2$  où  $S'_1 = S_1 - (S_1, 1)$ . Or

$$S = S_1 S_2 = S'_1 S_2 + (S_1, 1) S_2$$

Soit  $\psi$  la forme linéaire sur  $\mathbb{M}$  :

$$\psi(m_1, v, m_2) = (S_1, 1) \varphi_2(m_2)$$

Alors  $(\mathbb{M}, \mu, \varphi + \psi)$  est une représentation de  $S$  donc  $\mathbb{M}$  reconnaît  $S$ .  $\square$

Remarque 2. On pourra remarquer l'analogie de ces constructions avec celles de Schützenberger (1961, III. A.2 et 1965).

Définition 3. Une  $a$ -variété  $V$  est fermée par produit de Schützenberger si pour tous  $\mathbb{M}_1, \mathbb{M}_2 \in V$  on a aussi  $\mathbb{M}_1 \diamond \mathbb{M}_2 \in V$ .

Nous obtenons une première caractérisation des variétés fermées par produit

Théorème 1.  $\mathcal{V}$  est fermée par produit si et seulement si  $V$  est fermé par produit de Schützenberger.

Preuve. Si  $V$  est fermée par produit de Schützenberger,  $\mathcal{V}$  est fermée par produit, d'après le lemme 1. Réciproquement soit  $\mathcal{V}$  une  $s$ -variété non nulle fermée par produit. Soit  $V$  la  $a$ -variété associée et  $\mathbb{M}_1, \mathbb{M}_2 \in V$  et  $\mathbb{M} = \mathbb{M}_1 \diamond \mathbb{M}_2$ . Pour montrer que  $\mathbb{M} \in V$ , il suffit de montrer que toute série reconnue par  $\mathbb{M}$  est dans  $\mathcal{V}$  (lemme 7 du § 1). Soit donc  $X$  un alphabet,  $\mu : K\langle X \rangle \rightarrow \mathbb{M}$  un morphisme et  $\varphi$  une forme linéaire sur  $\mathbb{M}$ . Soit  $V = \mathbb{M}_1 \otimes \mathbb{M}_2$  et  $p_1, q, p_2$ , les projections de  $\mathbb{M}$  sur  $\mathbb{M}_1, V$  et  $\mathbb{M}_2$  respectivement ;  $p_1$  et  $p_2$  sont des homomorphismes d'algèbres, donc  $\mu_1 = p_1 \circ \mu$ ,  $\mu_2 = p_2 \circ \mu$  le sont aussi. Posons  $\nu = q \circ \mu$ . Soit  $\varphi_1, \psi$  et  $\varphi_2$  les restrictions de  $\varphi$  à  $\mathbb{M}_1, V$  et  $\mathbb{M}_2$  respectivement.

On a :

$$\varphi = \varphi_1 + \psi + \varphi_2$$

$$\mu = (\mu_1, \nu, \mu_2)$$

Par suite

$$\varphi \circ \mu = \varphi_1 \circ \mu_1 + \psi \circ \nu + \varphi_2 \circ \mu_2$$

Le premier et le troisième terme sont des séries dans  $\mathcal{V}$ , puisque reconnues par  $\mathcal{M}_1$  et  $\mathcal{M}_2$ . Il suffit donc de montrer que  $\psi \circ \nu \in \mathcal{V}$ . Or  $\psi$  est une somme finie de formes linéaires de la forme  $\psi_1 \otimes \psi_2$  où  $\psi_1$  et  $\psi_2$  sont des formes linéaires sur  $\mathcal{M}_1$  et  $\mathcal{M}_2$  respectivement. On peut donc supposer  $\psi = \psi_1 \otimes \psi_2$ . Or il existe un entier  $p$  tel que

$$\forall x \in X, \nu x = \sum_{1 \leq i \leq p} m_{x,i} \otimes n_{x,i} \quad (m_{x,i} \in \mathcal{M}_1, n_{x,i} \in \mathcal{M}_2)$$

On vérifie, par récurrence sur  $|w|$ , la formule :

$$\forall w \in X^*, \nu w = \sum_{\substack{w = u x v \\ u, v \in X^*, x \in X}} \mu_1 u \cdot \nu x \cdot \mu_2 v$$

Par suite

$$\nu w = \sum_i \sum_{w = u x v} \mu_1 u \cdot m_{x,i} \otimes n_{x,i} \cdot \mu_2 v$$

et

$$\psi \circ \nu w = \sum_i \sum_{w = u x v} \psi_1(\mu_1 u \cdot m_{x,i}) \psi_2(n_{x,i} \cdot \mu_2 v)$$

Soient  $S_{i,x}$  et  $T_{i,x}$  les séries ayant pour représentation  $(\mathcal{M}_1, \mu_1, \psi_1)$  et  $(\mathcal{M}_2, \mu_2, \psi_2)$  respectivement, avec

$$\psi_{1,i,x}(m_1) = \psi_1(m_1 \cdot m_{x,i}), \quad \psi_{2,i,x}(m_2) = \psi_2(n_{x,i} \cdot m_2)$$

On a  $S_{i,x}, T_{i,x} \in \mathcal{V}$  et l'on a

$$\begin{aligned}\psi \circ \nu \quad w &= \sum_{i,x} \sum_{w=u \times v} \psi_{1,i,x} (\mu_1 u) \psi_{2,i,x} (\mu_2 v) \\ &= \sum_{i,x} \sum_{w=u \times v} (S_{i,x}, u) (T_{i,x}, v) = \sum_{i,x} (S_{i,x} \times T_{i,x}, w)\end{aligned}$$

$$\text{Donc } \psi \circ \nu = \sum_{i,x} S_{i,x} \times T_{i,x}$$

Comme  $\mathcal{V}$  est fermée par produit et littérale (prop. 1), on a  $\psi \circ \nu \in \mathcal{V}$ .  $\square$

D'après un théorème de Schützenberger (1965) le monoïde syntactique d'un langage est *apériodique* (i.e. les groupes qu'il contient sont triviaux) si et seulement s'il appartient à l'algèbre de Boole fermée par produit engendrée par les lettres. Nous montrons pour les séries un résultat analogue.

Théorème 2. Soit  $S \in K \langle\langle X \rangle\rangle$  une série rationnelle. Les conditions suivantes sont équivalentes.

- (i) Tout quotient simple de  $\mathcal{M}_S$  est isomorphe à  $K$ .
- (ii) Toute représentation matricielle de  $\mathcal{M}_S$  est triangulable.
- (iii)  $S$  appartient à la sous-algèbre de  $K \langle\langle X \rangle\rangle$  engendrée par les lettres et les séries géométriques.

Ici l'auteur de ce travail se doit d'évoquer de nombreuses discussions qu'il a eues avec Jean-Eric Pin, il y a déjà deux ans (comme le temps passe !...), au cours desquelles se sont dégagées les notions d'algèbre syntactique et de variété de séries rationnelles (pour lesquelles JEP a servi pour le moins comme catalyseur) et auxquelles le théorème ci-dessus doit son existence. (JEP m'a fait soupçonner l'importance, au moins technique, des algèbres triangulables pour les séries "apériodiques").

Nous avons besoin de quelques lemmes. Si  $\mathbb{M}$  est une algèbre et  $\mu : \mathbb{M} \rightarrow K^{n \times n}$  un homomorphisme nous dirons que  $\mu$  est sous la forme (T) si  $\mu$  est triangulaire par blocs :

$$(T) \quad \mu = \begin{pmatrix} \mu_1 & x & \dots & x \\ 0 & \mu_2 & & \\ \vdots & & \ddots & \\ 0 & \dots & 0 & \mu_r \end{pmatrix}, \quad \mu_i : \mathbb{M} \rightarrow K^{n_i \times n_i}$$

Lemme 2. Soit  $\mathbb{M}$  une algèbre et  $\mu : \mathbb{M} \rightarrow K^{n \times n}$  un homomorphisme

- (i) On peut, par changement de base, mettre  $\mathbb{M}$  sous la forme (T) où les  $\mu_i$  sont des représentations irréductibles et les algèbres  $\mu_i(\mathbb{M})$  simples.
- (ii) Si  $\mu$  est injective et sous la forme (T) alors toute algèbre simple quotient de  $\mathbb{M}$  est quotient d'une des algèbres  $\mu_i(\mathbb{M})$ .

Rappelons qu'une sous-algèbre  $\mathbb{M}$  de  $K^{n \times n}$  est dite *irréductible* si les seuls sous-espaces de  $K^n$  qui sont stables sous toutes les matrices de  $\mathbb{M}$  sont 0 et  $K^n$ ; une représentation  $\mu : \mathbb{M} \rightarrow K^{n \times n}$  est dite *irréductible* si  $\mu(\mathbb{M})$  l'est.

Preuve. (i) Si  $\mu$  est irréductible,  $\mu$  est sous la forme (T). De plus,  $K^n$  devient un  $\mu(\mathbb{M})$ -module simple donc  $\mu(\mathbb{M})$  est une algèbre primitive de dimension finie, donc simple (Herstein, 1968, th. 2.1.4.). Si  $\mu$  n'est pas irréductible, on peut mettre  $\mu$ , par changement de base, sous la forme

$$\mu = \begin{pmatrix} \mu' & x \\ 0 & \mu'' \end{pmatrix}$$

et l'on conclut par récurrence.

- (ii) On peut supposer les  $\mu_i$  irréductibles, donc les  $\mu_i(\mathbb{M})$  simples. Soit  $I \subset \{1, \dots, r\}$  tels que les idéaux maximaux  $\text{Ker } \mu_j$  ( $j \in I$ )

soient deux à deux distincts et que pour tout  $i \in \{1, \dots, r\}$  il existe  $j \in I$  tel que  $\text{Ker } \mu_i = \text{Ker } \mu_j$ . Alors les idéaux  $\text{Ker } \mu_j$  ( $j \in I$ ) sont deux à deux étrangers donc l'homomorphisme canonique

$$\nu = (\mu_j)_{j \in I} : \mathbb{A} \rightarrow \prod_{j \in I} \mu_j \quad (\mathbb{A})$$

est surjectif (théorème chinois, voir Curtis-Reiner 1962, 18.18). Soit  $m \in \text{Ker } \nu$ . Alors pour tout  $i \in \{1, \dots, r\}$ ,  $\mu_i(m) = 0$ . Par suite,  $\mu(\text{Ker } \nu)$  est un idéal nilpotent et il en est de même pour  $\text{Ker } \nu$  puisque  $\mu$  est injectif. Donc  $\text{Ker } \nu$  est contenu dans le radical de  $\mathbb{A}$ , donc dans tout idéal maximal de  $\mathbb{A}$  et par suite tout quotient simple de  $\mathbb{A}$  est quotient de  $\prod_{j \in I} \mu_j(\mathbb{A})$  donc d'un des  $\mu_j(\mathbb{A})$ .  $\square$

Lemme 3. Soit  $S \in K\langle\langle X \rangle\rangle$  admettant la représentation  $(K^{n \times n}, \mu, \varphi)$  où  $\mu : K\langle X \rangle \rightarrow K^{n \times n}$  est sous la forme (T). Alors  $S$  appartient à l'algèbre engendrée par les lettres et les séries reconnues par les algèbres  $\mu_i(K\langle X \rangle)$ .

Preuve. Voir le lemme 4, §1, chap. VIII.  $\square$

Lemme 4. Soient  $\mathbb{A}_1, \mathbb{A}_2$  deux algèbres. Tout quotient simple de  $\mathbb{A}_1 \diamond \mathbb{A}_2$  est quotient de  $\mathbb{A}_1$  ou  $\mathbb{A}_2$ .

Preuve. Soit  $\mu : \mathbb{A}_1 \diamond \mathbb{A}_2 \rightarrow \mathbb{A}_1 \times \mathbb{A}_2$  l'homomorphisme surjectif défini par

$$\mu(m_1, v, m_2) = (m_1, m_2)$$

Il suffit de montrer que  $\text{Ker } \mu$  est nilpotent. Or

$$\text{Ker } \mu = \{ (0, v, 0) \mid v \in \mathbb{A}_1 \otimes \mathbb{A}_2 \}$$

donc  $(\text{Ker } \mu)^2 = 0$ . Par suite tout quotient simple de  $\mathbb{A}_1 \diamond \mathbb{A}_2$  est quotient de  $\mathbb{A}_1 \times \mathbb{A}_2$ , donc de  $\mathbb{A}_1$  ou  $\mathbb{A}_2$ .  $\square$

Preuve du théorème 2.

$\mathbb{M}_S$  est une algèbre de dimension finie et admet donc une représentation fidèle par matrices. D'où l'équivalence de (i) et (ii) sachant le lemme 2 et qu'une toute représentation irréductible

$$\mu : K \rightarrow K^{n \times n}$$

vérifie  $n = 1$ .

Remarquons que l'algèbre syntactique d'une lettre est isomorphe à

$$\left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in K \right\}$$

et donc que tout quotient simple de cette algèbre est isomorphe à  $K$ . Il en est de même pour les séries géométriques. Par suite, si  $S$  vérifie (iii),  $S$  peut être reconnue par une algèbre  $\mathbb{M}$  dont tous les quotients simples sont isomorphes à  $K$ , d'après le lemme 4 du § 1 et les lemmes 1 et 4 de ce paragraphe. On en déduit que  $\mathbb{M}_S$  est quotient d'une sous-algèbre  $\mathbb{M}'$  de  $\mathbb{M}$ . D'après le lemme 2,  $\mathbb{M}$  admet une représentation fidèle par matrices triangulaires et il en est donc de même de  $\mathbb{M}'$ . Par suite, les quotients simples de  $\mathbb{M}_S$ , qui sont aussi quotients de  $\mathbb{M}'$ , sont isomorphes à  $K$  (lemme 2). Que (ii) implique (iii) résulte du lemme 3.  $\square$

Perrot (1978) a montré qu'il existe une plus petite variété non triviale des langages fermée par produit, à savoir celle des langages aperiodiques. Nous prouvons ici un résultat analogue.

Proposition 2. *Il existe une plus petite s-variété  $V$  non nulle et fermée par produit. Elle est décrite dans le théorème 2.*

Preuve. Il suffit de vérifier que :

$$V = \{ \mathbb{M} \mid \text{tous les quotients simples de } \mathbb{M} \text{ sont isomorphes à } K \}$$

est une a-variété. Or, cela découle du lemme 2.  $\square$

Une pseudovariété de monoïdes finie  $V$  est appelée une *variété à groupes* (Perrot, 1978) si elle possède la propriété suivante : il existe une pseudovariété de groupes finis  $V'$  telle que :  $M \in V$  si et seulement si les groupes contenus dans  $M$  sont dans  $V'$ . Une telle variété est nécessairement fermée par produit (ibid.) mais la réciproque est fausse (Straubing, 1979).

Remarque 3. On avait pu croire que la notion analogue à celle de variété à groupes serait celle de  $a$ -variété déterminée par les corps qu'elle contient. Ceci est bien entendu absurde dans le cas où  $K$  est algébriquement clos, car dans ce cas tous ces corps sont isomorphes à  $K$ . Mais dans certains cas ( $K = \mathbb{Q}$  ou  $\mathbb{R}$  par exemple) on peut décrire en ces termes la  $a$ -variété de la proposition 2. Disons que le corps  $D$  est *contenu dans l'algèbre*  $\mathcal{M}$  si  $D$  est une partie de  $\mathcal{M}$  stable pour les opérations <sup>de  $\mathcal{M}$ , qui</sup> induisent une structure de corps. Alors les conditions suivantes sont équivalentes, si  $\mathcal{M}$  est de dimension finie et si  $K$  possède un surcorps  $L$  de dimension 2 sur  $K$  :

(i) Tous les quotients simples de  $\mathcal{M}$  sont isomorphes à  $K$ .

(ii) Tous les corps contenus dans  $\mathcal{M}$  sont isomorphes à  $K$ .

Si  $\mathcal{M}$  vérifie (i),  $\mathcal{M}$  admet une représentation fidèle par matrices triangulaires. Par suite, le polynôme minimal sur  $K$  de tout  $m \in \mathcal{M}$  se décompose entièrement sur  $K$ . Or, si  $m$  engendre un corps contenu dans  $\mathcal{M}$ , ce polynôme minimal est irréductible sur  $K$ ; par suite, il est de degré 1 et tout corps contenu dans  $\mathcal{M}$  est isomorphe à  $K$ .

Si  $\mathcal{M}$  vérifie (ii), soit  $R$  le radical de  $\mathcal{M}$ . Il existe une sous-algèbre  $\mathcal{M}'$  de  $\mathcal{M}$  telle que  $\mathcal{M}' \simeq \mathcal{M}/R$  (Kaplansky, 1969, th. 33, II. 4.). Or  $\mathcal{M}'$  est semi-simple donc  $\mathcal{M}' \simeq \mathcal{M}_1 \times \dots \times \mathcal{M}_n$  où les  $\mathcal{M}_i$  sont simples et tout quotient simple de  $\mathcal{M}$  est isomorphe à l'un des  $\mathcal{M}_i$ . Chaque  $\mathcal{M}_i$  est de la forme  $D^{n \times n}$  où  $D$  est un surcorps de  $K$ . D'après l'hypothèse on a

$D = K$  et  $n = 1$ , sinon  $\mathcal{M}$  contiendrait  $K^{2 \times 2}$  et donc un corps  $\neq K$  d'après l'hypothèse faite sur  $K$ , was zu beweisen war.

Nous allons montrer que si  $V$  est une  $a$ -variété correspondant à une  $s$ -variété  $\mathcal{V}$  fermée par produit, alors  $V$  est entièrement définie par les algèbres simples qu'elle contient.

Lemme 5. Soit  $V'$  une  $a$ -variété et  $V$  la classe des algèbres de dimension finie dont tous les quotients simples sont dans  $V'$ . Alors  $V$  est une  $a$ -variété.

Preuve. Cela découle du lemme 2.  $\square$

Définition 4.  $V$  est une variété à quotients s'il existe une  $a$ -variété  $V'$  telle que  $\mathcal{M} \in V$  si et seulement si tous les quotients simples de  $V$  sont dans  $V'$ . Notation :  $V = \diamond V'$ .

Remarque 4. Si  $V = \diamond V'$ , on a  $V = \diamond V''$  pour toute  $a$ -variété  $V''$  contenue dans  $V$  et contenant la  $a$ -variété engendrée par les algèbres simples contenues dans  $V$ .

Nous obtenons une nouvelle caractérisation des  $s$ -variétés fermées par produit.

Théorème 3. Une  $s$ -variété  $\mathcal{V}$  est fermée par produit si et seulement si la  $a$ -variété associée  $V$  est une variété à quotients.

Preuve. Si  $V$  est une variété à quotients,  $V$  est fermée par produit de Schützenberger (lemme 4) donc  $\mathcal{V}$  est fermée par produit (théorème 1).

Soit  $\mathcal{V}$  une  $s$ -variété fermée par produit. On a clairement  $V \subset \diamond V$ . Soit  $\mathcal{M} \in \diamond V$ . Alors  $\mathcal{M}$  admet une représentation fidèle sous la forme (T) où les algèbres  $\mu_i(\mathcal{M})$  sont simples, donc dans  $V$  (lemme 2) et par suite toute série reconnue par  $\mathcal{M}$  est dans  $\mathcal{V}$  (lemme 3) puisque  $\mathcal{V}$  est fermée par produit et contient les lettres (prop. 1). On en déduit que  $\mathcal{M} \in V$  (lemme 7 du § 1) donc  $\diamond V \subset V$ .  $\square$

# 5. VARIETES FERMEES PAR PRODUIT DE HADAMARD, DE HURWITZ .

Le produit de Hurwitz de deux mots  $u$  et  $v$  est un polynôme noté  $u \sqcup v$  et défini de la manière suivante :

$$u \sqcup v = \sum_{n \in \mathbb{N}} \sum_{\substack{u = u_1 \dots u_n \\ v = v_1 \dots v_n \\ u_2, \dots, u_n, v_1, \dots, v_{n-1} \neq 1}} u_1 v_1 u_2 \dots u_n v_n$$

Le produit de Hurwitz des séries  $S$  et  $T$  est encore noté  $S \sqcup T$  et il est défini par prolongement par linéarité : ce produit est commutatif et associatif (cf. Fliess, 1974a)

$$S \sqcup T = \sum_{u, v} (S, u) (T, v) u \sqcup v$$

Définition 1. (i) Une  $s$ -variété  $\mathcal{U}$  est fermée par produit de Hadamard (resp. de Hurwitz) si pour tout alphabet  $X$  et tous  $S, T \in X^* \mathcal{U}$  on a  $S \otimes T \in X^* \mathcal{U}$  (resp.  $S \sqcup T \in X^* \mathcal{U}$ ).

(ii) Une  $a$ -variété  $\mathcal{V}$  est fermée par produit tensoriel si pour tous  $\pi_1, \pi_2 \in \mathcal{V}$  on a  $\pi_1 \otimes_K \pi_2 \in \mathcal{V}$ .

Théorème 1. Soit  $\mathcal{V}$  une  $a$ -variété et  $\mathcal{U}$  la  $s$ -variété associée. Les conditions suivantes sont équivalentes.

- (i)  $\mathcal{V}$  est fermée par produit tensoriel
- (ii)  $\mathcal{U}$  est fermée par produit de Hadamard.
- (iii)  $\mathcal{U}$  est fermée par produit de Hurwitz.

Preuve. Pour (i)  $\Rightarrow$  (ii) et (i)  $\Rightarrow$  (iii), nous utilisons des constructions de Schützenberger (1962) et Fliess (1974 a). Si pour  $i = 1, 2$   $S_i \in K \langle\langle X \rangle\rangle$  est une série admettant la représentation  $(\pi_i, \mu_i, \varphi_i)$  alors  $S_1 \otimes S_2$  admet la représentation  $(\pi_1 \otimes \pi_2, \mu_1 \otimes \mu_2, \varphi_1 \otimes \varphi_2)$  et  $S_1 \sqcup S_2$  la représentation  $(\pi_1 \otimes \pi_2, \mu, \varphi_1 \otimes \varphi_2)$  avec

$$\mu = \mu_1 \otimes \mu_2 + \mu_1 \otimes \mu_2 + \mu_1 \otimes \mu_2 + \dots$$

(ii)  $\Rightarrow$  (i) Soient  $\mathbb{M}_1, \mathbb{M}_2 \in \mathcal{V}$  et  $\mathbb{M} = \mathbb{M}_1 \otimes \mathbb{M}_2$ . Pour montrer que  $\mathbb{M} \in \mathcal{V}$  il suffit de montrer que toute série reconnue par  $\mathbb{M}$  est dans (lemme 7 du § 1). Soit  $\mu : K\langle X \rangle \rightarrow \mathbb{M}$  et  $\varphi$  une forme linéaire sur  $\mathbb{M}$ . Il existe  $p \geq 1$  et pour tout  $x \in X$  des éléments  $m_{x,i} \in \mathbb{M}_1$  et  $n_{x,i} \in \mathbb{M}_2$  tels que

$$\mu x = \sum_{1 \leq i \leq p} m_{x,i} \otimes n_{x,i}$$

Soit  $Y$  l'alphabet  $Y = \{ y_{x,i} \}_{x \in X, 1 \leq i \leq p}$

et  $\nu$  le morphisme  $K\langle X \rangle \rightarrow K\langle Y \rangle$  défini par  $\nu(x) = \sum_{1 \leq i \leq p} y_{x,i}$

Soit  $\pi : K\langle Y \rangle \rightarrow \mathbb{M}$

$$y_{x,i} \mapsto m_{x,i} \otimes n_{x,i}$$

On a clairement  $\mu = \pi \circ \nu$  donc  $\varphi \circ \mu = \varphi \circ \pi \circ \nu$ . Il suffit donc de vérifier que  $\varphi \circ \pi \in \mathcal{V}$ . Or  $\varphi$  est somme de formes linéaires de la forme  $\varphi_1 \otimes \varphi_2$ . On peut donc supposer

$$\varphi = \varphi_1 \otimes \varphi_2$$

Mais alors  $\varphi \circ \pi$  est égal au produit de Hadamard des séries ayant pour représentation  $(\mathbb{M}_1, \pi_1, \varphi_1)$  et  $(\mathbb{M}_2, \pi_2, \varphi_2)$

avec  $\pi_1(y_{x,i}) = m_{x,i}$ ,  $\pi_2(y_{x,i}) = n_{x,i}$ .

Par suite  $\varphi \circ \pi \in \mathcal{V}$ .

(iii)  $\Rightarrow$  (ii) Soient  $S_1, S_2 \in X^* \mathcal{V}$ . Soit  $\bar{X}$  un alphabet en bijection avec  $X$ , distinct de  $X$ ; la bijection sera notée  $x \mapsto \bar{x}$ . Soit  $Y = X \cup \bar{X}$  et  $\mu : K\langle Y \rangle \rightarrow K\langle X \rangle$  défini par  $\mu x = x$  pour  $x \in X$  et  $\mu \bar{x} = 0$ . Alors  $S_1 \circ \mu \in Y^* \mathcal{V}$ .

Or  $S_1 \circ \mu = \sum_{w \in X^*} (S_1, w) w$

que nous notons encore  $S_1$ .

De la même manière  $\overline{S}_2 = \sum_{w \in X^*} (S_2, w) \overline{w} \in Y^*U$ .

Donc  $S = S_1 \circ \overline{S}_2 \in Y^*U$ .

Soit  $\nu : K\langle X \rangle \rightarrow K\langle Y \rangle$

$$x \mapsto x \overline{x}$$

Alors  $S \circ \nu \in X^*U$  et vérifie :  $\forall w \in X^*$

$$\begin{aligned} (S \circ \nu, w) &= (S, \nu w) = (S, x_1 \overline{x}_1 \dots x_n \overline{x}_n) = (S_1, w) (\overline{S}_2, \overline{w}) \\ &= (S_1, w) (S_2, w) = (S_1 \otimes S_2, w) \end{aligned}$$

si  $w = x_1 x_2 \dots x_n$ . Par suite  $S_1 \otimes S_2 \in X^*U$ .  $\square$

Théorème 2. Il existe une plus grande  $s$ -variété  $U$  fermée par produit de Hurwitz (de Hadamard). La  $a$ -variété  $V$  associée est définie par :  $M \in V$  si et seulement si tous ses quotients simples sont commutatifs (et sont donc des corps).

Il nous faut deux lemmes.

Lemme 1. Soit  $M$  une algèbre simple de dimension finie et non commutative. Il existe  $n \geq 2$  tel que  $K^{n \times n} < M \otimes M$ .

Preuve.  $M$  est de la forme  $D^{r \times r}$  où  $D$  est un surcorps de  $K$  (Herstein, 1968, th. 2.1.6). Si  $r \geq 2$ ,  $M$  contient  $K^{2 \times 2}$  et le lemme en découle. Si  $r = 1$ ,  $M = D$  et  $D$  est un corps non commutatif contenant  $K$  en son centre  $F$ . Soit  $L$  un sous-corps commutatif maximal de  $D$ . Alors

$$D \otimes_F L \simeq L^{n \times n}, \quad n = \dim_L(D) \geq 2$$

(ibid., corollaire au th. 4.2.1.). Comme  $K \subset F$  il existe un morphisme surjectif

$$D \otimes_K L \rightarrow D \otimes_F L$$

donc  $K^{n \times n} \subset L^{n \times n} \simeq D \underset{F}{\otimes} L \subset D \underset{K}{\otimes} D$ .  $\square$

Lemme 2. Soit  $V$  une  $a$ -variété fermée par produit tensoriel et contenant une algèbre simple  $\mathbb{M}$  non commutative. Alors  $V$  est la  $a$ -variété de toutes algèbres de dimension finie.

Preuve. D'après le lemme 1,  $V$  contient  $K^{n \times n}$  pour un  $n \geq 2$ . Or

$$K^{r \times r} \underset{K}{\otimes} K^{s \times s} \simeq K^{rs \times rs}$$

donc  $V = Alg$  (lemme 3 du § 2).  $\square$

Preuve du théorème 2. D'après le lemme 5 du § 4, la classe  $V$  décrite dans l'énoncé est une  $a$ -variété qui contient toute  $a$ -variété fermée par produit tensoriel et distincte de  $Alg$ . Il reste à vérifier que  $V$  est fermé par produit tensoriel. Mais ça découle du lemme 2 du § 4 et du fait que si

$$\mu_1 : \mathbb{M} \rightarrow K^{r \times r}, \quad \mu_2 : \mathbb{M} \rightarrow K^{s \times s}$$

sont deux morphismes d'image commutative, le morphisme

$$\mu_1 \otimes \mu_2 : \mathbb{M} \otimes \mathbb{M} \rightarrow K^{rs \times rs}$$

est aussi d'image commutative.  $\square$

Remarque 1. La  $s$ -variété décrite dans le théorème 2 est fermée par produit (d'après le th. 3 du § 4). De même la  $s$ -variété décrite dans le th. 2 du § 4 est fermée par produit de Hurwitz : cela découle du lemme 2 du § 4 et du fait que si  $\mu_1, \mu_2$  sont des représentations matricielles triangulables, il en est de même pour  $\mu_1 \otimes \mu_2$ . Ces deux  $a$ -variétés coïncident d'ailleurs si  $K$  est algébriquement clos.

Remarque 2. On conjecture, en théorie des variétés de langages, que toute variété de langages fermée par produit de Hurwitz et distincte de la variété

de tous les langages rationnels, est contenue dans celle des langages échangeables (voir Pin, 1980). Le théorème 2 peut s'interpréter comme l'analogue de cette conjecture. On notera en particulier que la commutativité y intervient de manière naturelle.

Remarque 3. Fliess (1974 a) , généralisant Lamperti (1958), définit les produits de Lamperti de deux séries : soient  $\alpha, \beta, \gamma$  des éléments de  $K$  ; on définit tout d'abord le produit de deux mots  $f$  et  $g$

$$f \mathcal{L}_{\alpha, \beta, \gamma} g = \sum \alpha^{n_1} \beta^{n_2} \gamma^{n_3} f_1 g_1 h_1 \dots f_k g_k h_k$$

où la somme est étendue aux  $f_i, g_i, h_i$  tels que

$$- f = f_1 h_1 \dots f_k h_k$$

$$- g = g_1 h_1 \dots g_k h_k$$

$$- f_2, \dots, f_k, g_1, \dots, g_{k-1} \neq 1$$

$$- n_1 = |f_1 \dots f_k|, \quad n_2 = |g_1 \dots g_k|, \quad n_3 = |h_1 \dots h_k|$$

(avec la convention  $0^0 = 1$ )

Ce produit s'étend par linéarité aux séries

$$S \mathcal{L}_{\alpha, \beta, \gamma} T = \sum_{f, g \in X^*} (S, f) (T, g) f \mathcal{L}_{\alpha, \beta, \gamma} g.$$

Fliess montre que le produit de Lamperti de deux séries rationnelles est encore une série rationnelle. La même méthode permet de montrer que si  $\mathcal{M}$  reconnaît  $S$  et  $\mathcal{M}'$  reconnaît  $T$  alors  $\mathcal{M} \otimes \mathcal{M}'$  reconnaît  $S \mathcal{L}_{\alpha, \beta, \gamma} T$ . On en déduit que si  $V$  est une  $a$ -variété fermée par produit tensoriel, la  $s$ -variété  $\mathcal{U}$  est fermée par tous les produits de Lamperti. La réciproque est également vraie et l'on a même : soit  $\mathcal{U}$  une  $s$ -variété fermée par le produit  $\mathcal{L}_{\alpha, \beta, \gamma}$  où  $\alpha, \beta, \gamma$  sont fixés et vérifient  $\gamma \neq 0$ , ou  $\alpha\beta \neq 0$ . Alors  $V$  est fermée par produit tensoriel. Il suffit de montrer que  $\mathcal{U}$  est fermée par

produit d'Hadamard. Or, si  $\alpha = \beta = 0$ ,  $\gamma \neq 0$  et  $\mathcal{L}_{\alpha, \beta, \gamma}$  vérifie

$$S \mathcal{L}_{\alpha, \beta, \gamma} T = \sum_w (S, w) (T, w) \gamma^{|w|} w$$

et si  $\nu : K\langle X \rangle \rightarrow K\langle X \rangle$  est défini par  $\nu x = \frac{1}{\gamma} x$ , alors  $S \ominus T =$

$(S \mathcal{L}_{\alpha, \beta, \gamma} T) \circ \nu$ . Si  $\alpha\beta \neq 0$ , alors on montre, comme pour l'implication

(iii)  $\Rightarrow$  (ii) du théorème 1, que  $S, T \in X^* \mathcal{U}$  implique

$$U = \sum_w (\alpha\beta)^{|w|} (S, w) (T, w) w \in X^* \mathcal{U}.$$

ce qui entraîne, avec  $\nu x = \frac{1}{\alpha\beta} x$ , que  $S \ominus T = U \circ \nu \in X^* \mathcal{U}$ .

On notera par ailleurs que si  $\alpha = \beta = 0$ ,  $\gamma = 1$ ,  $\mathcal{L}_{\alpha, \beta, \gamma}$  n'est autre que le produit d'Hadamard et que si  $\alpha = \beta = 1$ ,  $\gamma = 0$ , c'est le produit de Hurwitz.

## 6. VARIÉTÉS ÉQUATIONNELLES.

Eilenberg et Schützenberger ont introduit la notion de variété ultimement équationnelle de monoïdes et ont montré que toute pseudovariété de monoïdes finis est de la sorte (Eilenberg, 1976, th. V.2.1.). Ce résultat est à rapprocher du théorème de Birkhoff : toute variété (cette fois-ci, on autorise les produits infinis) d'algèbres (au sens de l'algèbre universelle) est équationnelle (mais ce n'est plus le cas pour les pseudovariétés).

Définition 1. (i) Une  $a$ -variété  $V$  est *équationnelle* s'il existe un alphabet (non nécessairement fini)  $\Sigma$  et un idéal  $I$  dans  $K\langle \Sigma \rangle$  tels que pour toute algèbre de dimension finie  $\mathcal{M}$  on a :  $\mathcal{M} \in V$  si et seulement si pour tout homomorphisme  $\mu : K\langle \Sigma \rangle \rightarrow \mathcal{M}$ , on a  $\mu(I) = 0$ .

(ii) Une  $s$ -variété  $V$  est *ultimement équationnelle* si  $V$  est réunion de variétés équationnelles.

Exemple 1. Contrairement à ce qui se passe pour les monoïdes finis, toute  $a$ -variété n'est pas ultimement équationnelle. Supposons en effet  $K$  infini et considérons la plus petite  $a$ -variété non nulle

$$V = \{ K^n \mid n \geq 0 \} \quad (\text{cf. § 2a}).$$

Supposons que  $V = \bigcup_{i \in I} V_i$  où les  $V_i$  sont équationnelles. Comme  $V_i \subset V$ , on a  $V_i = 0$  ou  $V_i = V$  et par suite  $V$  est équationnelle. Mais si  $\Sigma$  est un alphabet et  $P \in K\langle \Sigma \rangle$ , on a :  $\gamma(P) = 0$  pour tout  $n$  et tout morphisme  $\gamma: K\langle \Sigma \rangle \rightarrow K^n$  si et seulement si  $P$  est dans l'idéal  $I$  engendré par les commutateurs ( $K$  étant infini). Mais alors,  $V$  serait la  $a$ -variété de toutes les algèbres commutatives de dimension finie, ce qui n'est pas, comme le montre l'exemple

$$\mathcal{M} = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in K \right\}$$

Cependant, nous obtenons le

Théorème 1. Si  $K$  est fini, toute  $a$ -variété est ultimement équationnelle.

Pour démontrer ce théorème, nous nous inspirerons d'Eilenberg (1976, chap. 5, § 2), et nous utiliserons plusieurs lemmes.

Lemme 1. Soit  $\mathcal{M}$  une algèbre de dimension finie sur le corps fini  $K$  et  $\Sigma$  un alphabet fini. Soit  $I_{\mathcal{M}}$  l'idéal de  $K\langle \Sigma \rangle$  défini par :  $P \in I_{\mathcal{M}}$  si et seulement si pour tout morphisme  $\gamma : K\langle \Sigma \rangle \rightarrow \mathcal{M}$ ,  $\gamma(P) = 0$ . Alors  $K\langle \Sigma \rangle / I_{\mathcal{M}}$  est de dimension finie sur  $K$  et il existe  $n$  tel que  $K\langle \Sigma \rangle / I_{\mathcal{M}}$  soit isomorphe à une sous-algèbre de  $\mathcal{M}^n$ .

Preuve. On a  $I_{\mathcal{M}} = \bigcap_{\gamma} \text{Ker } \gamma$  où l'intersection est étendue à tous les morphismes  $\gamma : K\langle \Sigma \rangle \rightarrow \mathcal{M}$ . Comme  $K$  est fini,  $\mathcal{M}$  est fini, et il n'existe par suite qu'un nombre fini de tels morphismes. Par suite,  $I_{\mathcal{M}}$  est de codi-

mension finie. De plus, l'homomorphisme canonique

$$K\langle \Sigma \rangle / I_{\mathcal{M}} \rightarrow \prod_{\mathcal{V}} K\langle \Sigma \rangle / \text{Ker } \mathcal{V}$$

est injectif. Comme  $K\langle \Sigma \rangle / \text{Ker } \mathcal{V}$  s'injecte dans  $\mathcal{M}$ , la dernière assertion s'en déduit.  $\square$

Lemme 2. On suppose  $K$  fini. Soit  $\mathcal{M}$  une algèbre de dimension finie et  $\mathcal{V}$  la  $a$ -variété engendrée par  $\mathcal{M}$ . Alors  $\mathcal{V}$  est équationnelle.

Preuve. Soit  $\Sigma$  un alphabet infini et  $I$  l'idéal de  $K\langle \Sigma \rangle$  défini par

$$I = \bigcap_{\mathcal{V}} \text{Ker } \mathcal{V}$$

où l'intersection est étendue à tous les morphismes  $\mathcal{V} : K\langle \Sigma \rangle \rightarrow \mathcal{M}$ .

Alors on a

$$\mathcal{M}' \in \mathcal{V} \Leftrightarrow \forall \mu : K\langle \Sigma \rangle \rightarrow \mathcal{M}', \mu(I) = 0.$$

(donc  $\mathcal{V}$  est équationnelle).

En effet, si  $\mathcal{M}' \in \mathcal{V}$ ,  $\mathcal{M}'$  est quotient d'une sous-algèbre  $\mathcal{M}'_1$  de  $\mathcal{M}^n$  pour un  $n \geq 1$  (lemme 6 du § 1). Soit alors  $\mu : K\langle \Sigma \rangle \rightarrow \mathcal{M}'$ . Comme  $\mathcal{M}'$  est quotient de  $\mathcal{M}'_1$  et  $K\langle \Sigma \rangle$  libre, on peut factoriser  $\mu$  à travers  $\mathcal{M}'_1$  :

$$\begin{array}{ccc} K\langle \Sigma \rangle & \xrightarrow{\mu} & \mathcal{M}' \\ & \searrow \mathcal{V} & \nearrow \\ & \mathcal{M}'_1 & \end{array}$$

Mais alors, pour tout  $P \in K\langle \Sigma \rangle$ ,  $\mathcal{V}(P) = (\mathcal{V}_1(P), \dots, \mathcal{V}_n(P)) \in \mathcal{M}'^n$ , et les  $\mathcal{V}_i$  sont des morphismes  $K\langle X \rangle \rightarrow \mathcal{M}$ . Alors  $\mathcal{V}_i(I) = 0$ , donc  $\mathcal{V}(I) = 0$  et enfin  $\mu(I) = 0$ .

Réciproquement, si  $\mu(I) = 0$  pour tout morphisme  $\mu: K\langle \Sigma \rangle \rightarrow M'$ , soit  $\mu: K\langle \Sigma \rangle \rightarrow M'$  un morphisme surjectif et  $\Sigma'$  un sous-alphabet fini de  $\Sigma$  tel que  $\mu(K\langle \Sigma' \rangle) = M'$ . Soit  $\mu'$  la restriction de  $\mu$  à  $K\langle \Sigma' \rangle$  et  $I' = I \cap K\langle \Sigma \rangle$ . Alors  $\mu'(I') = 0$ , donc  $I' \subseteq \text{Ker } \mu'$  et par suite  $M'$  est quotient de  $K\langle \Sigma' \rangle / I'$ . Or, d'après le lemme 1,  $K\langle \Sigma' \rangle / I'$  s'identifie à une sous-algèbre de  $M^n$  pour un  $n \geq 1$ . Par suite  $M' \in V$ .  $\square$

Preuve du théorème 1. Soit  $V$  une  $a$ -variété. On a

$$V = \bigcup_{M \in V} V(M)$$

où  $V(M)$  est la  $a$ -variété engendrée par  $M$ , donc équationnelle (lemme 2). Par suite,  $V$  est ultimement équationnelle.  $\square$

Exemple 2. Supposons  $K$  fini et  $V$  la  $a$ -variété des algèbres  $K^n$ ,  $n \geq 0$ . Soit  $\Sigma$  un alphabet infini et  $I$  l'idéal de  $K\langle \Sigma \rangle$  engendré par les polynômes  $xy - yx$  et  $x^p - x$  ( $x, y \in \Sigma$ ) où  $p = \text{Card}(K)$ . Alors  $V$  est équationnelle, déterminée par l'idéal  $I$  (cf. preuve du lemme 2).

Exemple 3. (Jean-Eric Pin). On suppose  $K$  algébriquement clos de caractéristique nulle. Soit  $\Sigma$  un alphabet infini et  $I_n$  les idéaux de  $K\langle \Sigma \rangle$  définis récursivement par :

- $I_1$  est l'idéal engendré par les crochets de Lie  $[x, y]$  avec  $x, y \in \Sigma$ .
- $I_n$  est l'idéal engendré par les crochets de Lie  $[P, Q]$  avec  $P, Q \in I_{n-1}$ .

Soit  $V_n$  la  $a$ -variété équationnelle définie par  $I_n$  et  $V$  la  $a$ -variété ultimement équationnelle

$$V = \bigcup_{n \geq 1} V_n$$

Si  $\mathfrak{M} \in V$ , il existe  $n$  tel que  $\mathfrak{M} \in V_n$  et  $\mathfrak{M}$  admet une représentation fidèle par matrices triangulaires sur  $K$  (th. de Lie, voir Godement, 1966, ex. 27, § 34). Réciproquement, si  $\mathfrak{M}$  est ainsi, il est clair que  $\mathfrak{M} \in V_n$  pour  $n$  assez grand. Ainsi  $V$  est la  $a$ -variété décrite dans la proposition 2 du § 4 (qui coïncide, puisque  $K$  est algébriquement clos, avec celle du th. 2, § 5).

## CHAPITRE VI - SÉRIES DE PÓLYA

-----

Le point de départ de ce chapitre est une tentative d'étendre aux séries rationnelles en plusieurs variables non commutatives, une caractérisation, due à Pólya, des séries rationnelles d'une variable, à coefficients rationnels et qui ne font intervenir qu'un nombre fini de facteurs premiers : Pólya montre que ces séries sont inversibles dans l'algèbre d'Hadamard des séries rationnelles. Il se pose donc la double question de la caractérisation des séries Hadamard-inversibles (pour plusieurs variables non commutatives) et celle des séries vérifiant la condition de Pólya, et que j'ai appelées "séries de Pólya". Je n'ai pu résoudre ces problèmes dans le cas général. Sont présentés ici des résultats partiels, et des conjectures qui semblent raisonnables.

Monsieur Benzaghou a caractérisé les séries rationnelles d'une variable à coefficients dans un corps de caractéristique nulle qui sont Hadamard-inversibles : ces séries sont exactement les emboîtements de séries géométriques. J'étends ici au cas de la caractéristique quelconque ce beau théorème, et ce, par une preuve entièrement algébrique (th. 1, § 3), contrairement à celle de Monsieur Benzaghou, qui était analytique. Ceci dit, une formulation de ce résultat revient

à dire que, dans le cas d'une variable, les séries Hadamard-inversibles sont rationnelles non ambiguës, notion qui trace le cadre adéquat du problème en plusieurs variables. J'introduis cette notion (issuë de la théorie des langages) et l'étudie au § 1. Au § 2, j'étudie les séries de Pólya et prouve deux cas particuliers de ma conjecture (à savoir l'égalité entre séries de Pólya et séries rationnelles non ambiguës) : le cas où la série est échangeable et le cas où elle ne comporte qu'un seul facteur premier, très grand.

Dans ce chapitre, les alphabets sont supposés finis.

1 - SERIES RATIONNELLES NON AMBIGUES.

Nous définissons les opérations rationnelles non ambiguës.

Définition 1. Soit  $(S_i)_{i \in I}$  une famille de séries formelles de  $K \langle\langle X \rangle\rangle$ .

(i) On dit que la somme  $\sum S_i$  est non ambiguë si les langages  $\text{supp}(S_i)$  sont deux à deux disjoints.

(ii) On suppose  $I = \{1, \dots, n\}$ : On dit que le produit  $\prod_{1 \leq i \leq n} S_i$  est non ambigu si pour tout mot  $w$  il existe au plus une famille de mots  $(u_i)_{i \in I}$  telle que  $u_i \in \text{supp } S_i$  et  $w = u_1 u_2 \dots u_n$ .

(iii) Si  $S$  est une série propre, on dit que l'étoile  $S^*$  est non ambiguë si  $\text{supp}(S)$  est un code (i.e. la base d'un sous-monofide libre de  $X^*$ ).

Remarque 1. Si la somme  $\sum S_i$  est non ambiguë, la famille  $(S_i)$  est évidemment sommable (et même localement finie)... Par ailleurs, il est facile de voir que l'étoile  $S^*$  est propre si et seulement si la somme  $\sum_{n \geq 0} S^n$  est non ambiguë et si tous les produits  $S^n$  sont non ambiguës.

Définition 2. Les opérations rationnelles non ambiguës sont la somme finie non ambiguë, le produit non ambigu et l'étoile non ambiguë.

Définition 3. Une série formelle  $S \in K \langle\langle X \rangle\rangle$  est dite rationnelle non ambiguë si elle appartient au plus petit sous-ensemble de  $K \langle\langle X \rangle\rangle$  contenant  $K \langle X \rangle$  et fermé pour les opérations rationnelles non ambiguës.

Remarque 2. Une série rationnelle non ambiguë est rationnelle... Lorsque  $K$  est le demi-anneau de Boole, on retrouve la notion habituelle d'opérations rationnelles non ambiguës de langages. Rappelons à ce sujet que tout langage rationnel est rationnel non ambigu (cf. Eilenberg 1974, th. 8.2, chap. VII).

Définition 4. Soient  $A^1, \dots, A^n$  des matrices de taille quelconque à coeffi-

cients dans  $K$  telles que le produit  $A^1 \dots A^n$  soit défini. Le produit  $A^i$  est *non ambigu* si pour tout indice de ligne  $i$  de  $A^1$  et tout indice de colonne  $j$  de  $A^n$  il existe au plus un  $(n-1)$  uplet d'indices  $(i_1, \dots, i_{n-1})$  tels que  $A^1_{i, i_1}, A^2_{i_1, i_2}, \dots, A^n_{i_{n-1}, j} \neq 0$ .

Définition 5. Une représentation matricielle  $(\lambda, \mu, \gamma)$  est *non ambiguë* si pour tout  $n \geq 0$  et tous  $x_1, \dots, x_n \in X$  le produit  $\lambda, \mu x_1, \mu x_2 \dots, \mu x_n, \gamma$  est non ambigu.

Définition 6. Une série  $S \in K\langle\langle X \rangle\rangle$  est *reconnaissable non ambiguë* si  $S$  admet une représentation linéaire  $(\lambda, \mu, \gamma)$  non ambiguë.

Théorème 1. Une série est rationnelle non ambiguë si et seulement si elle est reconnaissable non ambiguë.

Preuve. Dire que la représentation  $(\lambda, \mu, \gamma)$  est non ambiguë revient exactement à dire que dans l'automate associé à  $(\lambda, \mu, \gamma)$ , pour tout mot  $w \in X^*$  il existe au plus un triplet  $(i, j, c)$  où  $i$  est un état initial,  $j$  un état final et  $c$  un chemin  $i \rightarrow j$  d'étiquette  $w$ . Moyennant cette remarque, le théorème se démontre comme le théorème de Kleene-Schützenberger (voir Eilenberg 1974, chap. VI, prop. 7.1, 7.8 et 7.9 et chap. VII, th. 5.1).  $\square$

Proposition 1. Soit  $S$  une série formelle.  $S$  est rationnelle non ambiguë si et seulement si il existe un alphabet  $Y$ , une fonction rationnelle  $\tau : X^* \rightarrow Y^*$  (i.e. une application partielle dont le graphe est une partie rationnelle de  $X^* \times Y^*$ ) et un morphisme  $\varphi : Y^* \rightarrow K$  (multiplicatif), tel que

$$\forall w \in X^*, (S, w) = \varphi \circ \tau w.$$

avec la convention  $\varphi(\emptyset) = 0$ . Si  $K$  est intègre (i.e.  $ab = 0$  implique  $a = 0$  ou  $b = 0$ ) on peut supposer  $\text{dom } \tau = \text{supp } S$  et que toute lettre de  $X$  intervient dans  $\text{Im } \tau$ .

Preuve. Soit  $S$  une série rationnelle non ambiguë et  $(\lambda, \mu, \gamma)$  une représentation matricielle non ambiguë de  $S$ . Soit  $Y$  un alphabet en bijection avec l'ensemble  $K'$  des coefficients non nuls des matrices  $\lambda$ ,  $\gamma$  et  $\mu x$  ( $x \in X$ ) : la bijection sera notée  $\varphi : Y \rightarrow K' \subset K \setminus 0$ . Soit  $(\bar{\lambda}, \bar{\mu}, \bar{\gamma})$  une nouvelle représentation matricielle, qu'on obtient en remplaçant dans les matrices  $\lambda$ ,  $\mu x$  et  $\gamma$  chaque élément non nul par son image par  $\varphi^{-1}$ . Alors  $(\bar{\lambda}, \bar{\mu}, \bar{\gamma})$  est non ambiguë : en effet, soient  $y_1, \dots, y_n \in Y$  et  $i_0, \dots, i_n$  tels que

$$\lambda_{i_0}, (\bar{\mu} y_1)_{i_0, i_1}, \dots, (\bar{\mu} y_n)_{i_{n-1}, i_n}, \gamma_{i_n} \in Y.$$

Alors leurs images par  $\varphi$  sont des éléments non nuls de  $K$ . De la non ambiguïté de  $(\lambda, \mu, \gamma)$  découle donc l'unicité du  $(n+1)$ -uplet  $(i_0, i_1, \dots, i_n)$ , donc la non-ambiguïté de  $(\bar{\lambda}, \bar{\mu}, \bar{\gamma})$ . Cette représentation définit donc une application partielle  $\tau : X^* \rightarrow Y^*$  qui vérifie clairement  $S = \varphi \circ \tau$ . D'après Berstel (1979, th. 4.5, chap. IV)  $\tau$  est une fonction rationnelle. On a clairement  $\text{supp } S \subset \text{dom } \tau$ . Si de plus  $K$  est intègre, alors  $w \in \text{dom } \tau$  implique  $(S, w) = \varphi \circ \tau w \neq 0$  (car  $0 \notin \varphi(Y)$ ) donc  $w \in \text{supp } S$ . Réciproquement, soient  $\varphi$ ,  $Y$  et  $\tau$  comme dans l'énoncé : il existe alors une représentation linéaire non ambiguë  $(\bar{\lambda}, \bar{\mu}, \bar{\gamma})$  dont chaque coefficient est soit 0, soit un mot sur  $Y$  (ibid). Remplaçons chaque entrée des matrices  $\bar{\lambda}$ ,  $\bar{\mu} x$  et  $\bar{\gamma}$  par son image par  $\varphi$  ; nous obtenons une représentation linéaire  $(\lambda, \mu, \gamma)$  qui est clairement non ambiguë. De plus  $(S, w) = \lambda \cdot \mu w \cdot \gamma$  pour tout mot  $w$  donc  $S$  est rationnelle non ambiguë.  $\square$

Corollaire 1. Si  $S$  est rationnelle non ambiguë, l'ensemble de ses coefficients est une partie rationnelle de  $K$  (multiplicatif). Elle est en particulier contenue dans un sous-monoïde de type fini de  $K$ .

Preuve. Ecrivons  $S = \varphi \circ \tau$  (prop. 1). Alors  $\tau(X^*)$  est une partie rationnelle de  $Y^*$  et par suite  $\varphi \circ \tau(X^*)$  est une partie rationnelle de  $K$ . Or,  $\text{Im}(S) = \varphi \circ \tau(X^*) \cup 0$  si  $\text{supp}(S) = \text{dom}(\tau) \neq X^*$  et  $\text{Im}(S) = \varphi \circ \tau(X^*)$  dans les autres cas.  $\square$

Corollaire 2. Si  $K$  est intègre, le support d'une série rationnelle non ambiguë est un langage rationnel.

$\square$

Proposition 2. On suppose  $K$  commutatif. Le produit d'Hadamard de deux séries rationnelles non ambiguës est une série rationnelle non ambiguë.

Preuve. Soit  $S_i = |(\lambda_i, \mu_i, \gamma_i)|$ ,  $i = 1, 2$  où  $(\lambda_i, \mu_i, \gamma_i)$  est une représentation matricielle non ambiguë. Soit  $(\lambda, \mu, \gamma)$  la représentation définie par :  $\lambda = \lambda_1 \otimes \lambda_2$ ,  $\mu = \mu_1 \otimes \mu_2$ ,  $\gamma = \gamma_1 \otimes \gamma_2$ . Soient  $x_1, \dots, x_n \in X$  et  $(i_0, j_0), \dots, (i_n, j_n)$  tels que

$$\lambda_{(i_0, j_0)}, \mu^{x_1}_{(i_0, j_0), (i_1, j_1)}, \dots, \mu^{x_n}_{(i_{n-1}, j_{n-1}), (i_n, j_n)}, \gamma_{(i_n, j_n)} \neq 0$$

Alors

$$\lambda_{i_0}, \mu^{x_1}_{i_0, i_1}, \dots, \mu^{x_n}_{i_{n-1}, i_n}, \gamma_{i_n} \neq 0$$

$$\text{et } \lambda_{j_0}, \mu^{x_1}_{j_0, j_1}, \dots, \mu^{x_n}_{j_{n-1}, j_n}, \gamma_{j_n} \neq 0$$

Par suite,  $(\lambda_1, \mu_1, \gamma_1)$  et  $(\lambda_2, \mu_2, \gamma_2)$  étant non ambiguës, les  $i$  et les  $j$  sont uniquement déterminés par  $x_1, \dots, x_n$ . Donc  $(\lambda, \mu, \gamma)$  est non ambiguë. Par ailleurs,  $K$  étant commutatif,  $S_1 \otimes S_2$  est reconnue par  $(\lambda, \mu, \gamma)$ .  $\square$

Corollaire 1. Soit  $S$  une série rationnelle non ambiguë et  $L$  un langage rationnel. Alors la série  $\sum_{w \in L} (S, w) w$  est rationnelle non ambiguë.

Preuve. La série  $\underline{L} = \sum_{w \in L} w$  est rationnelle non ambiguë, puisque tout langage rationnel est non ambigu (Eilenberg 1974, th. 8.2). Par suite  $\sum_{w \in L} (S, w)w = \underline{L} \odot S$  est rationnelle non ambiguë.  $\square$

Corollaire 2. Soit  $S$  une série rationnelle non ambiguë et  $P$  un polynôme. Alors  $S + P$  est une série rationnelle non ambiguë.

Preuve.  $\text{supp}(P)$  et  $L = X^* \setminus \text{supp}(P)$  sont des langages rationnels, et l'on a

$$S + P = S \odot \underline{L} + (S + P) \odot \underline{X^* \setminus L}$$

Cette somme est non ambiguë, le premier terme est une série rationnelle non ambiguë (cor. 1), et le second aussi, puisque c'est un polynôme.  $\square$

Proposition 3. Si  $X = \{x\}$ ,  $S \in K\langle\langle X \rangle\rangle$  est rationnelle non ambiguë si et seulement s'il existe  $m \geq 1$ ,  $a_0, \dots, a_m, b_0, \dots, b_m \in K$  tels que  $S$  diffère au plus par un polynôme de

$$S_1 = a_0(b_0 x^m)^* + a_1 x(b_1 x^m)^* + \dots + a_{m-1} x^{m-1} (b_{m-1} x^m)^*$$

ce qui s'écrit aussi, si  $K$  est un anneau

$$S_1 = a_0(1 - b_0 x^m)^{-1} + a_1 x(1 - b_1 x^m)^{-1} + \dots + a_{m-1} x^{m-1} (1 - b_{m-1} x^m)^{-1}$$

Preuve. Si  $S$  est de la forme indiquée,  $S$  est clairement non ambiguë. Réciproquement, les seules étoiles non ambiguës dans  $K[[x]]$  sont celles des séries de la forme  $(ax^n)^*$  ( $a \in K$ ,  $n \geq 1$ ). De plus, tout langage rationnel infini  $L$  dans  $x^*$  contient une progression arithmétique :  $x^{a+m\mathbb{N}} \subset L$  ( $m \geq 1$ ). Si  $H$  est un autre langage, alors la non ambiguïté du produit  $HL$  implique que  $x^p, x^q \in H$ ,  $p \neq q \Rightarrow p \not\equiv q \pmod{m}$ . A partir de là, il n'est pas très difficile de voir que  $S$  a la forme voulue.  $\square$

Remarque 1. La série  $S_1$  de la proposition ci-dessus est exactement ce que Benzaghoul (1970) appelle une *fonction de Pólya*.

## 2. SERIES DE POLYA.

Définition 1. Soit  $S \in \mathbb{Q} \langle\langle X \rangle\rangle$ . L'ensemble des facteurs premiers de  $S$ , noté  $P(S)$ , est l'ensemble des nombres premiers  $p$  tels qu'il existe un mot vérifiant :

$(S, w) = p^r \frac{a}{b}$ , où  $r, a, b$  sont des entiers non nuls et  $p$  ne divise ni  $a$  ni  $b$ .

Autrement dit,  $p \in P(S)$  si et seulement si  $v_p(\text{Im}(S) \setminus \{0\}) \neq 0$  ( $v_p$  est la valuation  $p$ -adique).

Exemple 1. Si  $S = \sum_{n \geq 0} n^2 x^n$ ,  $P(S)$  est égal à l'ensemble de tous les nombres premiers. Si  $S = \sum 2^n x^n$ ,  $P(S) = \{2\}$ .

Définition 2. Une série  $S \in \mathbb{Q} \langle\langle X \rangle\rangle$  est une *série de Pólya* si l'ensemble des facteurs premiers est fini.

La terminologie est empruntée à Pólya (1921) qui montre que toute série rationnelle d'une variable n'ayant qu'un nombre fini de facteurs premiers peut se mettre sous la forme "d'un nombre fini de progressions géométriques arithmétiquement emboîtées". De manière précise, si  $S$  est une telle série, il existe un entier  $m \geq 1$ , des nombres rationnels  $a_i$  et  $b_i$  ( $1 \leq i \leq m$ ) et un polynôme  $P$  tels que  $S$  soit égale à  $S_1 + P$  avec

$$S_1 = \frac{a_0}{1 - b_0 z^m} + z \frac{a_1}{1 - b_1 z^m} + \dots + z^{m-1} \frac{a_{m-1}}{1 - b_{m-1} z^m}$$

(voir aussi Benzaghoul, 1970, th. 1, chap. V). Par suite  $S$  est rationnelle ambiguë (prop. 3, § 1).









En outre, l'ensemble des facteurs premiers d'une série est fini si et seulement si l'ensemble de ses coefficients est contenu dans un sous-monoïde multiplicatif de type fini de  $\mathbb{Q}$ . Par suite (cor. 1 à la prop. 1, § 1)

Proposition 1. *Toute série rationnelle non ambiguë est une série de Pólya.*

Ceci nous amène à la

Conjecture 1. *Une série rationnelle est une série de Pólya si et seulement si elle est une série rationnelle non ambiguë.*

Outre le cas  $\text{card}(X) = 1$ , complètement élucidé par Pólya (1921), nous allons voir que la conjecture est vraie dans trois cas particuliers. Auparavant nous donnons quelques résultats qui vont dans le sens de la conjecture ci-dessus.

Proposition 2. (i) *Le support d'une série de Pólya rationnelle est un langage rationnel.*

(ii) *Si  $S$  est une série rationnelle avec  $P(S) = \{p\}$ , alors le langage  $\{w \in X^* \mid (S, w) > 0\}$  est rationnel.*

Preuve. (i) Par le critère d'Eisenstein (prop. 6, § 3, chap. I), on est ramené aux cas des séries à coefficients entiers. Mais alors, on peut utiliser la proposition 1 du § 5 chap. VII.

(ii) Il existe des entiers  $a$  et  $b$  tels que  $\forall w \in X^* \quad v_p(S, w) \geq a|w| + b$  (prop. 5 du § 3, chap. I). Par suite, la série  $T = \sum (S, w) p^{-a|w| - b} w$  est rationnelle à coefficients entiers, et  $P(T) = \{p\}$ . Il existe un entier  $a \geq 2$  tel que pour tous nombres entiers  $m$  et  $n \geq 0$  on n'a jamais

$$p^{11} \equiv -p^m \pmod{a}$$

En effet, si  $p > 3$ , on prend  $a = p - 1 > 2$  alors  $p \equiv 1$ , donc  $p^n + p^m \equiv 1 + 1 = 2$  qui n'est pas nul modulo  $a$ . Si  $p = 2$ , on prend

on prend  $a \equiv 7$  car l'équation

$$2^n + 1 \equiv 0 \pmod{7}$$

n'a pas de solutions. De même si  $p \equiv 3$ , on prend  $a \equiv 11$  car l'équation

$$3^n + 1 \equiv 0 \pmod{11}$$

n'a pas de solutions.

Soit  $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}/a\mathbb{Z}$  la projection canonique. Alors la série

$$\sum \varphi(T, w) w$$

est  $(\mathbb{Z}/a\mathbb{Z})$ -rationnelle. Par suite, les langages  $\{w \mid \varphi(T, w) = \alpha\}$  sont rationnels (voir Salomaa-Soittola, 1977, th. 2.1., chap. III), et de l'hypothèse sur  $a$  il s'ensuit que  $\{w \mid (T, w) > 0\} = \{w \mid (S, w) > 0\}$  est rationnel.  $\square$

Remarque 1. Il n'est pas difficile de montrer que si  $S$  est une série rationnelle non ambiguë, alors le langage

$$\{w \mid (S, w) > 0\}$$

est rationnel (cf. prop. 1, § 1).

Corollaire. Si  $S$  est une série de Pólya rationnelle, la série  $T$  définie par  $(T, w) = (S, w)$  si  $(S, w) \neq 0$ ,  $(T, w) = 1$  sinon, est une série de Pólya rationnelle et  $\text{supp}(T) = X^*$ .

Cela nous permet de ramener l'étude des séries de Pólya rationnelles à l'étude de celles qui n'ont aucun coefficient nul.

Preuve. Le langage  $L = X^* \setminus \text{supp}(S)$  est rationnel, donc  $T = S + \underline{L}$  est une série rationnelle et possède les propriétés ci-dessus.  $\square$

Proposition 3. Soit  $S$  une série de  $\mathbb{N}$ -série rationnelle. On suppose que  $P(S) = \{p_1, \dots, p_n\}$  et que

$$\forall w \in X^* \quad (S, w) = (\varepsilon, w) p_1^{(S_1, w)} \dots p_n^{(S_n, w)}$$

où  $(\varepsilon, w) \in \{0, 1, -1\}$  et où les  $S_i$  sont des séries à coefficients entiers. Soient  $t_1, \dots, t_n$  des indéterminées. Alors  $S$  est rationnelle non ambiguë si et seulement si la série (à coefficients dans  $\mathbb{Q}(t_1, \dots, t_n)$ )

$$T = \sum_{w \in X^*} (\varepsilon, w) t_1^{(S_1, w)} \dots t_n^{(S_n, w)} w$$

est rationnelle.

Preuve. Si  $S$  est rationnelle non ambiguë, écrivons  $S = \varphi \circ \tau$ , où  $\gamma, \varphi$  et  $\tau$  sont comme dans la prop. 1 du § 1. On peut supposer que toute lettre  $y$  de  $Y$  intervient dans un mot de  $\text{Im } \tau$  et que  $\text{dom } \tau = \text{supp}(S)$ . Soit  $y \in Y$ . Alors il existe  $u \in \text{dom } \tau$  tel que  $\tau u = ayb \Rightarrow 0 \neq (S, u) = \varphi(a) \varphi(y) \varphi(b)$ . Par suite, les seuls nombres premiers intervenant dans le nombre  $\varphi(y)$  sont  $p_1, \dots, p_n$ . Posons  $\psi(y) = \eta_y t_1^{k_1} \dots t_n^{k_n}$  si  $\varphi(y) = \eta_y p_1^{k_1} \dots p_n^{k_n}$  où  $\eta_y \in \{1, -1\}$ . Alors  $\psi$  se prolonge en un morphisme  $Y \rightarrow \mathbb{Q}(t)$  qui vérifie, pour tout mot  $w \in Y^*$

$$\psi(w) = \eta_w t_1^{k_1} \dots t_n^{k_n} \iff \varphi(w) = \eta_w p_1^{k_1} \dots p_n^{k_n}$$

Par suite, pour tout  $u \in X^*$

$$(T, u) = \psi \circ \tau(u)$$

et la série  $T$ , image par la transduction rationnelle  $\tau^{-1}$  de la série  $\mathbb{Q}(t)$ -rationnelle  $\sum \psi(w)w$ , est rationnelle (cf. Jacob, 1975).

Réciproquement, supposons que la série  $T$  soit rationnelle. Nous allons, dans un premier temps, faire l'hypothèse que  $(\varepsilon, w) = 1$  pour tout mot  $w$  et que  $T$  est  $\mathbb{Z}[t]$ -rationnelle. Soit

$$\varphi_i : \mathbb{Z}[t] \rightarrow \mathbb{Z}^{2 \times 2}$$

$$t_j \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ si } j = i \text{ et } \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ sinon.}$$

Alors la série

$$\varphi_i(T) = \sum_{w \in X^*} \begin{pmatrix} 1 & (S_i, w) \\ 0 & 1 \end{pmatrix} w$$

est  $\mathbb{Z}^{2 \times 2}$ -rationnelle. Par suite, la série  $\sum (S_i, w) w$  est  $\mathbb{Z}$ -rationnelle (voir cor. 2 à la prop. 1, § 3, chap. I). Mais d'après le cor. à la prop 5, § 3, chap. I, il existe une constante  $C_i$  telle que

$$\forall w \in X^* , |(S_i, w)| \leq C_i |w|$$

dans la série  $S_i$  est à croissance linéaire. Mais alors,  $S_i$  est  $\mathbb{N}$ -rationnelle (Reutenauer 78, th. 3), donc l'ensemble

$$\{(w, t_i^{(S_i, w)}) \mid w \in X^*\}$$

est une partie rationnelle du monoïde  $X^* \times t_i^*$  (ibid. th. 4). L'application

$$X^* \rightarrow t_i^*$$

$$w \mapsto t_i^{(S_i, w)}$$

est donc une fonction rationnelle, et par suite il existe une représentation linéaire non ambiguë  $(\lambda_i, \mu_i, \gamma_i)$  telle que  $t_i^{(S_i, w)} = \lambda_i \cdot \mu_i w$  (voir Berstel, 79, th. 4.5, chap. IV). Mais dans cette représentation il suffit de remplacer  $t_i$  par  $p_i$  pour obtenir une représentation linéaire non ambiguë de la série  $\sum p_i^{(S_i, w)} w$  qui est donc rationnelle non ambiguë. La série  $S$ , étant égale au produit d'Hadamard de ces séries, est aussi rationnelle non ambiguë (prop. 2 du § 1).

Dans le cas général, on se ramène d'abord à  $S \in \mathbb{Z}\langle X \rangle$  en utilisant le critère d'Eisenstein (prop. 6, § 3, chap. I). Ensuite, constatant que  $T$  est  $\mathbb{Z}[t]$ -rationnelle (d'après le th. 2 du § 1 et la remarque 2 (ii) du chap. IV) on obtient, par application du morphisme  $\mathbb{Z}[t] \rightarrow \mathbb{Z}$  qui aux  $t_i$  associe 1, que la série

$$\bar{S} = \sum (\varepsilon, w) w$$

est rationnelle. Par conséquent (voir le cor. 4 au th. 1, § 3, chap. I) les langages  $L^+ = \{w \mid (S, w) > 0\}$ ,  $L^- = \text{supp}(S) \setminus L^+$  sont rationnels. Or  $S = (S \circ \underline{L}^+) + (S \circ \underline{L}^-)$  et la somme est non ambiguë. On est donc ramené au cas où  $S$  a tous ses coefficients non négatifs. Enfin, par application du corollaire à la proposition 2, on est ramené à  $\text{supp}(S) = X^*$ .  $\square$

Corollaire. Soient  $S$  et  $T$  comme dans l'énoncé de la proposition 3. Alors  $S$  est rationnelle non ambiguë si et seulement si la matrice de Hankel

$$((T, uv))_{u, v \in X^*}$$

est de rang fini.

Preuve. En effet, une série est rationnelle si et seulement si sa matrice de Hankel est de rang fini (Fliess, 1974, th. 2.1.1.).  $\square$

Ceci permet de donner une autre formulation à la conjecture. Appelons *matrice de Hankel* une matrice  $H$  infinie indicée par un monoïde libre de type fini telle que pour tous mots  $u$  et  $v$ ,  $H_{u,v}$  ne dépende que du mot  $uv$ . La conjecture suivante est équivalente à la conjecture 1.

Conjecture 2. Soit  $H$  une matrice de Hankel à coefficients dans  $\mathbb{Q}$  telle que l'ensemble de ses facteurs premiers soit  $\{p_1, \dots, p_n\}$ . Si  $H'$  est obtenue en remplaçant chaque coefficient  $\pm p_1^{k_1} \dots p_n^{k_n}$  par le monôme  $\pm t_1^{k_1} \dots t_n^{k_n}$

(où les  $t_i$  sont transcendants), alors  $H$  est de rang fini si et seulement si  $H'$  est de rang fini.

La proposition suivante donne une réponse partielle à la conjecture.

Proposition 4. Soit  $S$  une série de Pólya rationnelle de rang  $< n$  telle que

$$\text{Im}(S) \subset 0 \cup \{q^r \mid r \in \mathbb{Z}\}$$

où  $q$  est un entier  $\geq 2$ . Si  $q \geq n!$   $S$  est rationnelle non ambiguë.

La démonstration s'appuie sur les lemmes suivants.

Lemme 1. Si  $a_1, \dots, a_k, b_1, \dots, b_k$  sont des entiers non négatifs,  $q \geq k$ , et

$$q^{a_1} + q^{a_2} + \dots + q^{a_k} = q^{b_1} + q^{b_2} + \dots + q^{b_k}$$

alors  $k = 1$  et il existe une permutation telle que  $\forall i, a_i = b_{\sigma(i)}$

Preuve. Nous montrons qu'il existe un  $i$  et un  $j$  tel que  $a_i = b_j$ . On peut conclure alors par récurrence. Nous pouvons faire l'hypothèse

$$a_1 \leq a_2 \leq \dots \leq a_k \quad \text{et} \quad b_1 \leq b_2 \leq \dots \leq b_k$$

Si  $a_1 = b_1$ , nous avons fini. Sinon, l'on a par exemple  $a_1 < b_1$ . Soit  $i$  tel que

$$a_1 = a_2 = \dots = a_i < a_{i+1}$$

$$\text{Alors} \quad i q^{a_1} \equiv 0 \pmod{q^{a_1+1}}$$

Par suite,  $q$  divise  $i$ , ce qui est absurde puisque  $1 \leq i \leq k < q$ .  $\square$

Lemme 2. Soit  $A = (\varepsilon_{i,j} t^{r_{i,j}})$  une matrice d'ordre  $n$  avec  $\varepsilon_{i,j} \in \{0, 1, -1\}$  et  $B$  la matrice  $(\varepsilon_{i,j} t^{r_{i,j}})$  où  $t$  est transcendant. Si  $q \geq n!$ , alors  $\det(A) = 0$  implique  $\det(B) = 0$ .

Preuve. Le fait que  $\det(A) = 0$  s'écrit de la manière suivante :

$$0 = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{1 \leq i \leq n} q^{r_{i,\sigma(i)}} \varepsilon_{i,\sigma(i)}$$

Notons A l'ensemble des  $\sigma \in \mathfrak{S}_n$  tels que  $\varepsilon(\sigma) \prod_{1 \leq i \leq n} \varepsilon_{i,\sigma(i)} = 1$  et B son complémentaire. Alors l'égalité ci-dessus s'écrit

$$\sum_{\sigma \in A} q^{r_{1,\sigma(1)} + \dots + r_{n,\sigma(n)}} = \sum_{\sigma \in B} q^{r_{1,\sigma(1)} + \dots + r_{n,\sigma(n)}}$$

Mais  $\text{Card}(A), \text{card}(B) < n! \leq q$ , donc d'après le lemme 1, la même égalité a lieu lorsqu'on remplace  $q$  par  $t$ . Par suite,  $\det(B) = 0$ .  $\square$

Remarque 2. Est-ce que le lemme 2 est encore vrai sans l'hypothèse  $q \geq n!$  ?

Pour  $n = 2$ , c'est trivial ; pour  $q = 2$  et  $n = 3$ , on peut montrer que c'est vrai. Pour  $q = 2$  et  $n = 4$ , des essais par ordinateur ont montré qu'il existe de telles matrices A qui ne sont pas "triviales" (i.e. aucune ligne n'est multiple d'une autre et de même pour les colonnes), par exemple :

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & 4 & 2 & 1 \\ 4 & 2 & 1 & 4 \\ 1 & 1 & 4 & 2 \end{pmatrix}$$

Preuve de la proposition 4. Soit T la série définie par  $(T, w) = \varepsilon t^r$  si  $(S, w) = \varepsilon q^r$  où  $t$  est une indéterminée ( $\varepsilon = 0, 1$  ou  $-1$ ). Tout déterminant d'ordre  $n$  extrait de la matrice de Hankel de S est nul ; il en est donc de même pour ceux de T (lemme 2). Par suite, S est rationnelle non ambiguë (cor. à la prop. 3).  $\square$

Nous terminons ce paragraphe par un théorème de E. Birger (1972), qui donne une réponse affirmative à la conjecture 1 dans le cas des séries échangeables

et des séries dont le support est un langage borné. Les résultats obtenus par Birger sont plus précis que la formulation que nous allons en donner ; ils n'ont jamais été publiés et sont restés à l'état de manuscrit. Birger avait préparé une note au Comptes-Rendus de l'Académie des Sciences, mais sa mort prématurée en a empêché la publication ...

Rappelons qu'un langage  $L \subset X^*$  est dit *borné* s'il existe des mots  $w_1, \dots, w_n$  tels que

$$L \subset w_1^* w_2^* \dots w_n^*$$

Théorème (Birger) Soit  $S$  une série de Pólya rationnelle. Si  $S$  est échelonnée ou si  $\text{supp}(S)$  est un langage borné, alors  $S$  est rationnelle non ambiguë.

La preuve que nous donnons diffère sensiblement de la preuve originale. Nous utilisons le critère de rationalité du § 3, chap. III. Pour cela, nous avons besoin du

Lemme 3. Soient  $p_1, \dots, p_r$  des nombres premiers et  $t_1, \dots, t_r$  des indéterminées. A toute série  $S = \sum a_n x^n$  telle que  $P(S) \subset \{p_1, \dots, p_r\}$  nous associons la série  $\bar{S} = \sum \bar{a}_n x^n$  définie par

$$\bar{a}_n = \varepsilon t_1^{k_1} \dots t_r^{k_r} \text{ si } a_n = \varepsilon p_1^{k_1} \dots p_r^{k_r}$$

avec  $\varepsilon = -1, 0$  ou  $1$ .

Soit  $Q \in \mathbb{Q}[x]$ . Il existe  $\bar{Q} \in \mathbb{Q}(t)[x]$  tel que : pour toute série rationnelle  $S$  vérifiant  $P(S) \subset \{p_1, \dots, p_r\}$  et  $Q \circ S = 0$ , on a  $\bar{Q} \circ \bar{S} = 0$ .

Pour la définition de l'opération  $Q \circ S$ , on pourra se reporter au chap. I, et § 9).

Preuve. Nous utilisons le résultat suivant, dû à Pólya (1921) et qui, comme il le fait remarquer, est le point important ("Springende Punkt") de la démonstration du théorème rappelé au début de ce paragraphe : si la série rationnelle  $S$  est une série de Pólya et possède plus d'une racine, alors il existe deux racines distinctes de  $S$  dont le quotient est une racine de l'unité.

Soit  $k$  la multiplicité de  $0$  comme racine de  $Q$ . Soit  $N$  l'entier donné par la proposition 3 du § 9, chap. I. ( $N$  ne dépend que de  $Q$ ). Soit  $\bar{Q}_1 \in Q(t)[x]$

le produit des polynômes de la forme

$$x - \varepsilon t_1^{k_1} \dots t_r^{k_r}$$

tels que  $\varepsilon p_1^{k_1} \dots p_r^{k_r}$  soit racine de  $Q^{(N)}$ , avec  $\varepsilon = 0, -1$  ou  $1$ .

$$\bar{Q} = x^k \bar{Q}_2 \quad \text{avec} \quad \bar{Q}_2 = \bar{Q}_1(x^N).$$

Soit  $S$  une série rationnelle comme dans l'énoncé. Nous supposons dans un premier temps que  $S$  est régulière. Soient  $S_0, \dots, S_{N-1}$  telles que  $S$  soit égale à l'emboîtement de  $S_0, \dots, S_{N-1}$  (cf. prop. 3, § 9, chap. I). Les séries  $S_k$  vérifient  $P(S_k) \subset \{p_1, \dots, p_r\}$  et  $Q^{(N)} \circ S_k = 0$ ; de plus, les racines  $\neq 0$  de  $Q^{(N)}$  engendrent un groupe abélien libre, donc  $S_k$  n'a qu'une seule racine, qui est de multiplicité 1 (Pólya 1921); par suite; cette racine est de la forme

$$\varepsilon p_1^{k_1} \dots p_r^{k_r}$$

donc  $\bar{Q}_1 \circ \bar{S}_k = 0$ . D'où

$$\bar{Q}_2 \circ S = 0.$$

Si  $S$  n'est pas régulière,  $x^k \circ S$  est régulière et vérifie les hypothèses.

Donc

$$0 = \bar{Q}_2 \circ \overline{(x^k \circ S)} = \bar{Q}_2 \circ (x^k \circ \bar{S}) = \bar{Q} \circ \bar{S}$$

Preuve du théorème. Soit  $S$  une série de Pólya rationnelle. Nous lui associons une série  $T$  comme dans la proposition 3. Il suffit de montrer que  $T$  est  $Q(t)$ -rationnelle. Or, si  $S$  est échangeable,  $T$  l'est aussi et nous pouvons utiliser le théorème 3 du § 3, chap. III. Soit  $w \in X^*$  et  $Q$  le polynôme caractéristique de la matrice  $\mu w$ , où  $(\lambda, \mu, \gamma)$  est une représentation linéaire de  $S$ . Nous associons à  $Q$  un polynôme  $\bar{Q}$  comme dans le lemme 2. Soient  $u, v$  des mots. La série

$$S_1 = \sum (S, u w^n v) x^n$$

vérifie  $P(S_1) \subset P(S) = \{p_1, \dots, p_r\}$  et  $Q \circ S_1 = 0$ . Par suite,  $\bar{Q} \circ \bar{S}_1 = 0$ ; or

$$\bar{S}_1 = \sum (T, u w^n v) x^n$$

On peut donc appliquer le théorème cité.

Maintenant, si  $S$  est une série dont le support est contenu dans  $x_1^* x_2^* \dots x_n^*$  (avec  $X = \{x_1, \dots, x_n\}$ ),  $S$  peut être prolongée en une série rationnelle

échangeable  $S_1$  (Fliess, 1974, prop. 2.2.10).

D'après ce qui précède, la série  $T_1$  associée à  $S_1$  est rationnelle, donc  $T = T_1 \circ (\underline{x}_1^* \dots \underline{x}_n^*)$  l'est aussi.

Enfin, si le support de  $S$  est contenu dans  $w_1^* \dots w_n^*$ , soit  $Y$  un alphabet à  $n$  lettres :  $Y = \{y_1, \dots, y_n\}$  et  $\varphi$  le morphisme  $Y^* \rightarrow X^*$ ,  $\varphi(y_i) = w_i$ . Alors la série  $S_1$  sur  $Y$  définie par

$$(S_1, w) = (S, \varphi(w))$$

est rationnelle. Soit  $L$  une partie rationnelle de  $Y$  contenue dans  $y_1^* \dots y_n^*$  et telle que  $\varphi$  induise une bijection

$$L \mapsto w_1^* \dots w_n^*$$

(l'existence de  $L$  est assurée par Eilenberg, 1974, th. 7.1, chap. IX). La série  $S_2 = S_1 \circ L$  est rationnelle, de Pölya et son support est contenu dans  $y_1^* \dots y_n^*$ . Par suite, la série  $T_2$  associée à  $S_2$  est rationnelle. Or,  $\Psi$  restreint à  $\text{supp}(S_2) = \text{supp}(T_2)$  est injectif et  $T = \Psi(T_2)$ . Par suite  $T$  est rationnelle (voir le th. 1, § 3, chap. VII).  $\square$

### 3. SUR L'INVERSE DE HADAMARD

Dans ce paragraphe,  $K$  est un corps commutatif.

Rappelons que le produit de Hadamard de deux séries  $S$  et  $T \in K \langle\langle X \rangle\rangle$  est la série

$$S \circ T = \sum_{w \in X^*} (S, w) (T, w) w$$

Avec ce produit, l'ensemble des séries rationnelles devient une algèbre commutative (cf. chap. I, § 3, prop. 2) que nous appelons *l'algèbre de Hadamard des séries rationnelles*. Son élément neutre est la série dont tous les coefficients valent 1.

Rappelons qu'un élément d'une algèbre est dit *pseudo-régulier* s'il appartient à un groupe contenu dans le demi-groupe multiplicatif de l'algèbre.

Définition 1. Nous disons qu'une série rationnelle est *Hadamard-inversible* (resp. *Hadamard sous-inversible*) si elle est inversible (resp. pseudo-régulière) dans l'algèbre de Hadamard des séries rationnelles.

Lemme 1. Les idempotents de l'algèbre de Hadamard des séries rationnelles sont exactement les séries caractéristiques de langages rationnels.

Preuve. Si  $A$  est un langage rationnel,  $\underline{A}$  est une série rationnelle et  $\underline{A} \circ \underline{A} = \underline{A}$  (cf. prop. 4, § 3, chap. I).

Si  $S$  est un idempotent, pour tout mot  $w$ ,  $(S, w)$  est idempotent dans  $K$ , donc  $(S, w) = 0$  ou  $1$ . Par suite,  $S = \underline{A}$ , où  $A$  est un langage rationnel (cf. cor. 4 au th. 1, § 3, chap. I).  $\square$

Lemme 2. *Le support d'une série rationnelle Hadamard-sous-inversible est un langage rationnel.*

Preuve. Soit  $S$  une telle série et  $T$  l'élément neutre d'un groupe contenant  $S$  et contenu dans l'algèbre des séries rationnelles. On a  $S \odot T = S$ , donc  $\text{supp}(S) \subset \text{supp}(T)$ . De plus,  $S \odot S^{-1} = T$  donc  $\text{supp}(T) \subset \text{supp}(S)$ . Par suite  $\text{supp}(S) = \text{supp}(T)$  est rationnel (lemme 1).  $\square$

Lemme 3. *Une série rationnelle  $S$  est Hadamard sous-inversible si et seulement s'il existe un langage rationnel  $A$  et une série rationnelle Hadamard-inversible  $T$  tels que  $S = \underline{A} \odot T$ .*

Preuve. Si  $S = \underline{A} \odot T$  comme ci-dessus, soit  $T^{-1}$  l'inverse de  $T$ . Alors

$$S \odot (\underline{A} \odot T^{-1}) = \underline{A} \text{ et } \underline{A} \odot S = S$$

donc  $S$  appartient à un groupe contenu dans l'algèbre d'Hadamard des séries rationnelles : son élément neutre est  $\underline{A}$  (qui est une série rationnelle puisque  $A = \text{supp } S$  est rationnelle) et l'inverse de  $S$  est  $\underline{A} \odot T^{-1}$ . Réciproquement, si  $S$  est Hadamard-sous-inversible,  $A = \text{supp}(S)$  est un langage rationnel. Soit  $B = X^* \setminus A$  : c'est un langage rationnel, donc  $\underline{B}$  est une série rationnelle. Alors  $S + \underline{B}$  est Hadamard-inversible. En effet, soit  $\bar{S}$  l'inverse de  $S$  dans le groupe contenant  $S$ .

$$\text{On a } \text{supp } S = \text{supp } \bar{S} = A \text{ et } S \odot \bar{S} = \underline{A}.$$

$$\text{Donc } (S + \underline{B}) \odot (\bar{S} + \underline{B}) = \underline{A} + \underline{B} = \underline{X}^*.$$

$$\text{De plus, } S = (S + \underline{B}) \odot \underline{A}.$$

Proposition 1. *Toute série rationnelle non ambiguë est Hadamard-sous-inversible.*

Preuve. Soit  $S = \varphi \circ \tau$  où  $\varphi$ ,  $\tau$  et  $Y$  sont comme dans la prop. 1 du § 1,  $\text{supp}(S) = \text{dom}(\tau)$  et où toute lettre  $y \in Y$  intervient dans un mot de  $\text{Im } \tau$  : on a donc, pour un  $w \in X^*$  et  $a, b \in Y$   $\tau w = ayb \Rightarrow 0 \neq (S, w) = \varphi(a) \varphi(y) \varphi(b)$  donc  $\varphi(y) \neq 0$ . Par suite, pour tout mot  $u \in Y^*$ ,  $\varphi(u) \neq 0$  et par suite, il existe un morphisme  $\psi : Y^* \rightarrow K$  tel que  $\varphi(u) \psi(u) = 1, \forall u \in Y^*$ . Alors la série  $T = \psi \circ \tau$  vérifie  $S \odot T = \text{supp } S$  et  $T$  est rationnelle (prop. 1, § 1). Donc  $S$  est Hadamard-sous-inversible.  $\square$

Ce résultat nous amène à poser la

Conjecture. *Une série rationnelle est Hadamard sous-inversible si et seulement si elle est rationnelle non ambiguë.*

Il suffirait, d'après le lemme 3 et le corollaire 1 à la prop. 2 du § 1, de montrer que toute série rationnelle Hadamard-inversible est non ambiguë. Nous allons voir que la conjecture est vraie dans le cas des séries d'une variable : pour cela nous étendons au cas des corps de caractéristique quelconque un théorème de Benzaghoul (1970, th 3, chap. IV) qui l'avait établi pour les corps de caractéristique nulle.

Théorème 1. *Si  $S = \sum a_n x^n$  est une série rationnelle Hadamard-inversible, il existe  $m \geq 1$ , des  $a_0, \dots, a_{m-1}, b_0, \dots, b_{m-1}$  dans  $K$  tels que  $S$  diffère par un polynôme de la série*

$$\sum_{0 \leq i \leq m-1} a_i x^i (1 - b_i x^m)^{-1}$$

Remarque 1. Si  $S$  est comme ci-dessus, elle est rationnelle non ambiguë, d'après la prop. 3 du § 1.

La preuve du théorème 1 que nous allons faire est entièrement algébrique (contrairement à celle de Benzaghoul, qui est analytique).

Preuve (i) Soit  $T$  une série rationnelle telle que  $S \odot T = \sum x^n$ . D'après la proposition 4 du § 9, chap. I, il existe des séries rationnelles régulières  $S'$  et  $T'$  telles que  $S - S'$  et  $T - T'$  soient des polynômes. Alors  $S' \odot T' - \sum x^n$  est une série rationnelle régulière et un polynôme, donc, d'après la proposition 5 du § 9, chap. I,  $S' \odot T' = \sum x^n$ . On est donc ramené au cas où  $S$  et  $T$  sont régulières.

(ii) D'après la proposition 3 du § 9, chap. I, il existe un entier  $N$  et des séries rationnelles  $S_0, \dots, S_{N-1}, T_0, \dots, T_{N-1}$  telles que pour tout  $k$ , le couple  $(S_k, T_k)$  soit normal et que  $S$  (resp.  $T$ ) soit égal à l'emboîtement des séries  $S_0, \dots, S_{N-1}$  (resp.  $T_0, \dots, T_{N-1}$ ). On a alors, pour tout  $k$  :

$$S_k \odot T_k = \sum x^n. \text{ On est donc ramené au cas où le couple } (S, T) \text{ est normal.}$$

(iii) Si le couple  $(S, T)$  est normal et si  $S \odot T = \sum x^n$ , nous montrons qu'il existe  $\alpha$  et  $a$  dans  $K$  tels que  $S = \alpha \sum a^n x^n$ .

Rappelons d'abord le fait suivant : si  $G$  est un groupe abélien libre et  $A$  un anneau commutatif intègre, les seuls éléments inversibles de l'algèbre

$A[G]$  sont de la forme  $ag$ , où  $a$  est inversible dans  $A$  et  $g \in G$ .

Soient  $\lambda_1, \dots, \lambda_r$  les racines de  $S$  et  $\mu_1, \dots, \mu_s$  celles de  $T$ . Les  $\lambda_i$  et les  $\mu_j$  engendrent un groupe abélien libre  $G$ . Si  $K$  est de caractéristique nulle (resp. de caractéristique non nulle) il existe, dans une extension de  $K$ , des polynômes  $P_1(t), \dots, P_r(t), Q_1(t), \dots, Q_s(t)$  (resp. des éléments  $P_1, \dots, P_r, Q_1, \dots, Q_s$ ) tels que

$$S = \sum_{n \geq 0} (\lambda_1^n P_1(n) + \dots + \lambda_r^n P_r(n)) x^n$$

$$T = \sum_{n \geq 0} (\mu_1^n Q_1(n) + \dots + \mu_s^n Q_s(n)) x^n$$

$$(\text{resp. } S = \sum (\lambda_1^n P_1 + \dots + \lambda_r^n P_r) x^n$$

$$T = \sum (\mu_1^n Q_1 + \dots + \mu_s^n Q_s) x^n$$

Soit  $A$  l'anneau commutatif intègre  $K[t]$  (resp.  $K$ ). Comme  $S \otimes T = \sum x^n$ , on a, dans l'algèbre  $A[G]$

$$(\lambda_1 P_1(t) + \dots + \lambda_r P_r(t))(\mu_1 Q_1(t) + \dots + \mu_s Q_s(t)) = 1$$

d'après la proposition 1 du § 9, chap. I.

$$(\text{resp. } (\lambda_1 P_1 + \dots + \lambda_r P_r) (\mu_1 Q_1 + \dots + \mu_s Q_s) = 1$$

d'après la proposition 2 du § 9, chap. I.)

Par suite, d'après la remarque ci-dessus,  $r = 1$ ,  $P_1(t) = P_1$  est constant, donc

$$S = P_1 \sum \lambda_1^n x^n \quad \square$$

Remarque 1. Un autre cas où la conjecture est vraie est celui des séries  $\mathbb{Q}$ -rationnelles échangeables ou de support borné : si une telle série est Hadamard-inversible, on voit facilement, en utilisant le critère d'Eisenstein (voir prop. 6, § 3, chap. I), que c'est une série de Pólya, et l'on est ramené au théorème de Birger (§ 2).



## CHAPITRE VII - SUPPORTS

-----

Ce chapitre concerne les langages qui sont supports de séries rationnelles. Nous commençons par donner une preuve simple du théorème d'itération de Jacob, en utilisant une propriété combinatoire des mots, établie par Schützenberger ; cette méthode donne aussi une preuve plus courte du théorème de Jacob sur les demigroupes de type fini de matrices, à savoir : dans tout produit assez long de matrices, on peut trouver un produit aussi long qu'on le veut de matrices qui appartiennent à un même groupe. Au deuxième paragraphe, nous étendons le lemme d'itération en un lemme "à la Ogden" en utilisant le résultat suivant : dans tout produit assez long d'éléments d'une algèbre de dimension finie, on peut trouver un élément qui appartient à un groupe contenu dans le monoïde multiplicatif de cette algèbre. Au paragraphe suivant nous utilisons le lemme d'itération pour établir que la famille des langages qui sont supports d'une série  $K$ -rationnelle (où  $K$  est un demi-anneau contenu dans  $R$ ) est un cône rationnel fermé pour les opérations rationnelles ("full A F L"). Au paragraphe 4 nous énonçons deux conjectures, dont l'une prétend

que si deux langages complémentaires sont supports de séries rationnelles, alors ils sont l'un et l'autre rationnels. Nous la prouvons dans le cas des séries d'une variable (ce qui n'est nouveau qu'en caractéristique non nulle ; le cas de la caractéristique nulle se ramène au théorème de Skolem-Mahler-Lech) et nous montrons, dans le cas général, que le monoïde syntactique de tels langages est un monoïde de torsion (ce qui implique leur rationalité s'ils sont échangeables).

1. LE THEOREME D'ITERATION DE JACOB.

Nous supposons, dans ce paragraphe, que  $K$  est un corps commutatif.

Théorème 1 (G. Jacob, 197X). Soit  $S \in K\langle X \rangle$  une série rationnelle. Il existe un entier  $N$  tel que pour tout mot  $w \in \text{supp}(S)$ , pour toute factorisation  $w = aub$  où  $|u| \geq N$ , il existe une factorisation  $u = u_1 u_2 u_3$  telle que

$$a u_1 u_2^* u_3 b \cap \text{supp}(S) \text{ est infini.}$$

Nous allons donner une preuve simplifiée de ce résultat. Pour cela, nous utilisons, comme l'a fait Jacob, la notion de matrice pseudo-régulière. Rappelons qu'un élément  $m$  d'un anneau est dit *pseudo-régulier* s'il existe un groupe contenu dans le demi-groupe multiplicatif de cet anneau et contenant  $m$ .

Nous faisons agir toute matrice  $m \in K^{n \times n}$  à droite sur l'espace vectoriel  $K^n$ .

Lemme 1. Soit  $m \in K^{n \times n}$ . Les conditions suivantes sont équivalentes :

- (i)  $m$  est un élément pseudo-régulier de l'anneau  $K^{n \times n}$
- (ii) Il existe des matrices  $m_1, m_2$  telles que  $m = m_2 m_1$  et  $\text{rang}(m_1) = \text{rang}(m_1 m_2 m_1)$ .
- (iii) Le noyau et l'image de  $m$  sont supplémentaires.
- (iv)  $m$  est nulle ou inversible, ou semblable à une matrice de la forme

$$\begin{pmatrix} m' & 0 \\ 0 & 0 \end{pmatrix} \text{ où } m' \in K^{n' \times n'} \text{ est inversible}$$

$$\text{et } 0 < n' < n$$

- (v) Le polynôme minimal  $P(\lambda)$  de  $m$  n'est pas divisible par  $\lambda^2$ .

Une partie de ces équivalences se trouve dans Ranum (1909), et une autre dans Jacob (197X). Nous en faisons cependant la démonstration, pour l'agrément du lecteur.

Preuve. (i)  $\Rightarrow$  (ii) Soit  $e$  l'élément neutre du groupe contenant  $m$  et  $m$  l'inverse de  $m$  dans ce groupe.

$$\text{on a} \quad m e m m' = m \quad \text{donc}$$

$$\text{donc} \quad \text{rang}(m) = \text{rang}(m e m m') \leq \text{rang}(m e m) \leq \text{rang}(m)$$

$$\text{Donc} \quad \text{rang}(m) = \text{rang}(m e m) \quad \text{et} \quad e m = m.$$

$$(ii) \Rightarrow (iii) \quad \text{On a} \quad \text{Im}(m_1) \cap \text{Ker}(m_2 m_1) = 0, \quad \text{donc} \quad \text{Im}(m_1) \cap \text{Ker}(m) = 0$$

$$\text{De plus} \quad \text{rang}(m_1) = \text{rang}(m_1 m_2 m_1) \leq \text{rang}(m_2 m_1) \leq \text{rang}(m_1)$$

$$\text{donc} \quad \text{rang}(m_1) = \text{rang}(m_2 m_1). \quad \text{Comme} \quad \text{Im}(m_2 m_1) \subset \text{Im}(m_1)$$

$$\text{on a} \quad \text{Im}(m_1) = \text{Im}(m_2 m_1) = \text{Im}(m).$$

$$\text{Par suite} \quad \text{Im}(m) \cap \text{Ker}(m) = 0$$

$$(iii) \Rightarrow (iv) \quad \text{Si} \quad \text{Ker}(m) = 0 \quad \text{ou} \quad \text{Im}(m) = 0, \quad (iv) \quad \text{est vérifié.}$$

Si non  $\text{Im}(m)$  et  $\text{Ker}(m)$  sont des espaces supplémentaires et la restriction de  $m$  à  $\text{Im}(m)$  est un automorphisme de  $\text{Im}(m)$ . Par changement de base adapté à la somme directe  $K^n = \text{Im}(m) \oplus \text{Ker}(m)$ , on obtient la forme voulue.

(iv)  $\Rightarrow$  (v) Si  $m = 0$  ou  $m$  est inversible, (v) est vérifié. Sinon, soit  $Q(\lambda)$  le polynôme minimal de  $m'$ . Alors  $Q(0) \neq 0$  et  $P(\lambda) = \lambda Q(\lambda)$ .

(v)  $\Rightarrow$  (iv) Si  $P(\lambda) = \lambda$  ou  $P(0) \neq 0$ , (iv) est vérifié. Sinon,  $P(\lambda) = \lambda Q(\lambda)$  où  $Q$  est non constant et  $Q(0) \neq 0$ . Alors  $K^n = \text{Ker}(m) \oplus \text{Ker } Q(m)$  et ces sous-espaces sont stables sous  $m$ . De plus  $Q(0) \neq 0$  implique que la restriction de  $m$  à  $\text{Ker } Q(m)$  en est un automorphisme. Par changement de base adapté à cette somme directe, on obtient

(iv)  $\Rightarrow$  (i) C'est clair.  $\square$

Lemme 2. Soient  $m \in K^n \times n$ ,  $\lambda \in K^1 \times n$ ,  $\gamma \in K^n \times 1$  et soit  $(p_k)$  la suite :  $p_k = \lambda \cdot m^k \cdot \gamma$ . Si  $m$  est pseudo-régulière et  $p_1 \neq 0$ , il existe une infinité de  $k$  tels que  $p_k \neq 0$ .

Preuve. Soit  $\lambda^r + \alpha_1 \lambda^{r-1} + \dots + \alpha_{r-1} \lambda + \alpha_r$  le polynôme minimal de la matrice  $m$ . On a, d'après la proposition 1,  $\alpha_r \neq 0$  ou  $\alpha_{r-1} \neq 0$ . La suite  $(p_k)$  vérifie la formule de récurrence :

$$\forall k \in \mathbb{N}, p_{k+r} + \alpha_1 p_{k+r-1} + \dots + \alpha_{r-1} p_{k+1} + \alpha_r p_k = 0$$

Soit  $k \geq 1$ . Si  $p_k \neq 0$ , il existe  $j \geq k$  tel que  $p_j \neq 0$ . En effet, si  $\alpha_r \neq 0$ , cela découle de la relation ci-dessus. Sinon,  $\alpha_r = 0$  et  $\alpha_{r-1} \neq 0$  et l'on a  $p_{k-1+r} + \alpha_1 p_{k-2+r} + \dots + \alpha_{r-1} p_k = 0$  et il existe  $j \in \{k+1, \dots, k-1+r\}$  tel que  $p_j \neq 0$ . On conclut par récurrence.  $\square$

Théorème 2. (Jacob 1978). Soit  $X$  un alphabet fini et  $n, p$  des entiers positifs. Il existe un entier  $N$  tel que pour tout homomorphisme  $\mu : X^* \rightarrow K^{n \times n}$ , pour tout mot  $w$  de longueur au moins  $N$ , il existe des mots non vides  $w_1, \dots, w_p$  tels que  $w$  contienne en facteur  $w_p w_{p-1} \dots w_1$  et que les matrices  $\mu w_1, \dots, \mu w_p$  appartiennent à un même groupe contenu dans  $K^{n \times n}$ .

Pour démontrer ce résultat, nous employons une méthode différente de celle de Jacob. Elle s'appuie sur un lemme combinatoire de Schützenberger. Nous avons besoin d'une définition.

Définition 1. Les quasi-puissances sont des mots particuliers, définis récursivement de la manière suivante : tout mot non vide est une quasi-puissance d'ordre 0 ; une quasi-puissance d'ordre  $n \geq 1$  est un mot de la forme  $uvu$  où  $u$  est une quasi-puissance d'ordre  $n-1$ .

Exemple. Si  $u \neq 1$ ,  $uvuwuvu$  est une quasi-puissance d'ordre 2.

Lemme 3. (Schützenberger, 1961 à IV.5). Soit  $X$  un alphabet fini et  $r \geq 1$ .

Il existe un entier  $N$  tel que tout mot de longueur au moins  $N$  contienne en facteur une quasi-puissance d'ordre  $n$ .

Preuve. Soit  $d = \text{Card}(X)$ ,  $C_0 = 1$  et par récurrence  $C_{k+1} = C_k(1+d^{C_k})$ .

Alors tout mot de longueur au moins  $C_k$  contient en facteur une quasi-puissance d'ordre  $k$ .

En effet, c'est clair si  $k = 0$ . Soit  $k \geq 0$  et  $w$  un mot de longueur  $\geq C_{k+1}$ . Alors  $w$  contient en facteur un mot de la forme

$$u_1 u_2 \dots u_{d'}, \quad \text{avec} \quad d' = 1 + d^{C_k}$$

et  $\forall i, |u_i| = C_k$ . Le nombre de mots de longueur  $C_k$  étant égal à  $d^{C_k}$ , deux des  $u_i$  sont égaux et  $w$  contient en facteur un mot de la forme  $uvu$  avec  $|u| = C_k$ ; par récurrence,  $u$  contient en facteur une quasi-puissance d'ordre  $k$ , soit  $u' : u = au'b$ . Alors  $w$  contient la quasi-puissance d'ordre  $k+1$   $u'b v au'$ . Il ne reste plus qu'à poser  $N = C_n$ .  $\square$

Preuve du théorème 2. Soit  $r = (p+1)(n+1)$  et  $N$  l'entier du lemme 3.

Soit  $\mu : X^* \rightarrow K^{n \times n}$  un homomorphisme et  $w$  un mot de longueur  $\geq N$ . Alors  $w$  contient en facteur une quasi-puissance d'ordre  $r$ , que nous notons  $u_r$ ; il existe donc des mots  $u_0 \neq 1, u_1, \dots, u_{r-1}, v_1, \dots, v_r$  tels que

$$\forall i \in \{1, \dots, r\}, \quad u_i = u_{i-1} v_i u_{i-1}$$

On a (en écrivant  $\text{rg}(u)$  au lieu de  $\text{rg}(\mu u)$ ) :

$$n \geq \text{rg}(u_{i-1}) \geq \text{rg}(u_{i-1} v_i u_{i-1}) = \text{rg}(u_i)$$

Il existe donc  $i$  tel que :

$$\text{rg}(u_i) = \text{rg}(u_{i+1}) = \text{rg}(u_{i+2}) = \dots = \text{rg}(u_{i+p})$$

Pour simplifier l'écriture, nous faisons un changement d'indice et posons  $i = 0$ .

$$\text{rg}(u_0) = \text{rg}(u_1) = \dots = \text{rg}(u_p) = k$$

Nous vérifions l'existence de mots non vides  $w_1, w_2, \dots, w_p$  tels que

$$\forall i, 1 \leq j \leq p, u_j = u_0 w_j w_{j-1} \dots w_1$$

Posons en effet  $w_1 = v_1 u_0$ , alors  $u_1 = u_0 w_1$ .

Supposons construits  $w_1, \dots, w_{j-1}$ . Alors

$$u_j = u_{j-1} v_j u_{j-1} = u_0 w_{j-1} w_{j-2} \dots w_1 v_j u_0 w_{j-1} w_{j-2} \dots w_1$$

Il suffit donc de poser  $w_j = w_{j-1} w_{j-2} \dots w_1 v_j u_0$ .

On a, pour tout  $j, 1 \leq j \leq p$  :

$$k = \text{rg}(u_j) \leq \text{rg}(w_j) \leq \text{rg}(u_0) = k$$

donc les  $w_j$  ont tous même rang  $k = \text{rg}(u_0)$ . De plus,  $\text{Ker}(w_{j-1}) \subset \text{Ker}(w_j)$  donc  $\text{Ker}(w_{j-1}) = \text{Ker}(w_j)$  et  $\text{Im}(w_j) \subset \text{Im}(u_0)$  donc  $\text{Im}(w_j) = \text{Im}(u_0)$  (en écrivant  $\text{Ker}(u)$  au lieu de  $\text{Ker}(\mu u)$  et de même pour  $\text{Im}$ ). Les matrices  $\mu w_j$  ont donc toutes même noyau, égal à  $\text{Ker}(w_1)$ , et toutes même image, égale à  $\text{Im}(u_0)$ . De plus,  $\text{rg}(u_1) = \text{rg}(u_0 w_1) = \text{rg}(u_0)$ , donc

$$\text{Im}(u_0) \cap \text{Ker}(w_1) = 0$$

L'espace  $K^n$  est donc somme directe de  $\text{Im}(u_0)$  et  $\text{Ker}(w_1)$ , et par changement de base adaptée à cette somme directe, chaque matrice  $\mu w_j$  s'écrit

$$\begin{pmatrix} m_j & 0 \\ 0 & 0 \end{pmatrix}$$

où  $m_j$  est inversible. Comme

$$u_p = u_0 w_p w_{p-1} \dots w_1 \text{ est facteur de } w$$

le théorème s'en déduit.  $\square$

Remarque 1. Comme le montre la preuve, le théorème 2 est encore vrai si  $K$  est un corps gauche. Il en est d'ailleurs de même du théorème 1 : Jacob, dans sa preuve originelle, donne une version non commutative du lemme 2.

Preuve du théorème 1. Soit  $(\lambda, \mu, \gamma)$  une représentation linéaire de la série  $S$ , de dimension  $n$  et  $p = 1$ . Soit  $N$  l'entier du théorème 2. Alors pour tous mots  $w, a, u, b$ , comme dans l'énoncé  $u$  s'écrit  $u = u_1 u_2$  où  $u_2 \neq 1$  et  $\mu u_2$  est pseudo-régulière. La suite

$$p_k = \lambda \mu a u_1 \mu u_2^k \mu u_3 b \gamma$$

vérifie donc les hypothèses du lemme 2, puisque  $p_1 = (S, w) \neq 0$ . Il existe donc une infinité de  $k$  tels que  $p_k \neq 0$  et le théorème en découle.  $\square$

## 2. UN LEMME D'ITERATION "A LA OGDEN".

Dans ce paragraphe,  $K$  désigne un corps commutatif.

Nous allons montrer que l'existence d'une matrice pseudo-régulière dans un produit de matrices n'est pas liée à la finitude de l'alphabet. De manière précise nous prouvons le théorème 2 du paragraphe précédent, sous l'hypothèse supplémentaire  $p = 1$ , mais sans l'hypothèse que  $X$  soit fini. Nous pourrions en déduire un lemme d'itération pour les séries rationnelles, "à la Ogden", comme il en existe aussi pour les langages rationnels (cf. Berstel, 1979).

Théorème 1. Soit  $n$  un entier  $\geq 1$ . Il existe un entier  $N = N(n)$  tel que pour tout alphabet (non nécessairement fini)  $X$ , pour tout homomorphisme  $\mu : X^* \rightarrow K^{n \times n}$ , tout mot de longueur  $w$  au moins  $N$  a en facteur un mot  $v \neq 1$  tel que  $\mu v$  soit une matrice pseudo-régulière.

Ce théorème admet la formulation équivalente suivante :

Théorème 1'. Soit  $n$  un entier  $\geq 1$ . Il existe un entier  $N = N(n)$  tel que pour toute famille  $(m_i)_{1 \leq i \leq N}$  de matrices d'ordre  $n$ , il existe  $i, j$ ,  $1 \leq i, j \leq N$  tels que la matrice  $m_i \dots m_j$  soit pseudo-régulière.

Remarque 1. Nous verrons que

$$N(n) = \prod_{1 \leq i \leq n} \left[ \binom{n}{i} + 1 \right]$$

On a  $N(n) \leq 2^{n^2}$  et  $N(1) = 1$ ,  $N(2) = 3$ ,  $N(3) = 16$ . On peut montrer directement qu'on aurait pu choisir  $N(2) = 2$ ,  $N(3) = 9$ . La borne que nous donnons est donc loin d'être la meilleure possible.

Le résultat ci-dessus admet le corollaire suivant.

Corollaire. Soit  $\mathcal{M}$  une algèbre de dimension finie. Il existe un entier  $N$  (ne dépendant que de la dimension de  $\mathcal{M}$ ) tel que : pour toute famille  $(m_i)_{1 \leq i \leq N}$  d'éléments de  $\mathcal{M}$ , il existe  $i, j$ ,  $1 \leq i \leq j \leq N$  tels que  $m_i \dots m_j$  soit un élément pseudo-régulier de  $\mathcal{M}$ .

Preuve. Si  $\dim(\mathcal{M}) = n$ ,  $\mathcal{M}$  admet une représentation fidèle par matrices d'ordre  $n$ . On peut donc supposer :  $\mathcal{M} \subset K^{n \times n}$ . D'après le théorème 1', il reste donc à montrer que si  $m \in \mathcal{M}$  est pseudo-régulier dans  $K^{n \times n}$ ,  $m$  l'est aussi dans  $\mathcal{M}$ . Mais  $m$  s'écrit, après changement de base,

$$m = \begin{pmatrix} m' & 0 \\ 0 & 0 \end{pmatrix}$$

où  $m' \in GL_{n'}(K)$ . Soit  $I_{n'}$  la matrice identité d'ordre  $n'$  et

$$I' = \begin{pmatrix} I_{n'} & 0 \\ 0 & 0 \end{pmatrix}$$

Soit  $P(\lambda) = \lambda^k + \alpha_1 \lambda^{k-1} + \dots + \alpha_{k-1} \lambda + \alpha_k$  le polynôme minimal de  $m'$ . On a  $\alpha_k \neq 0$  et

$$0 = m'^k + \alpha_1 m'^{k-1} + \dots + \alpha_{k-1} m' + \alpha_k I_n,$$

donc  $0 = m^k + \alpha_1 m^{k-1} + \dots + \alpha_{k-1} m + \alpha_k I'.$

Donc  $I' \in \mathcal{M}$ . Soit

$$\bar{m} = -\alpha_k^{-1} (\alpha_{k-1} I' + \alpha_{k-2} m + \dots + \alpha_1 m^{k-2} + m^{k-1})$$

Comme  $mI' = I'm = m$ , on a  $\bar{m}I' = I'\bar{m} = \bar{m}$  et  $m\bar{m} = \bar{m}m = I'$ . De plus,  $\bar{m} \in \mathcal{M}$ , donc  $m$  et  $\bar{m}$  engendrent un groupe contenu dans  $\mathcal{M}$  et  $m$  est pseudo-régulier.  $\square$

Nous avons besoin d'un lemme combinatoire, proche d'un lemme de Jacob (1978)

Lemme 1. Soit  $X$  un alphabet (non nécessairement fini),  $n, k_0, \dots, k_n$  des entiers  $\geq 1$  et  $r: X^* \rightarrow \{0, 1, \dots, n\}$  une application vérifiant :  
 $\forall u, v, w \in X^*, r(uvw) \leq r(v)$ . Pour tout mot  $w$  de longueur au moins  $k_0 k_1 \dots k_n$ , il existe  $p, 0 \leq p \leq n$ , tel que  $w$  a un facteur de la forme  $w_1 w_2 \dots w_{k_p}$  avec  $\forall i, w_i \neq 1$  et  $\forall i \leq j, r(w_i \dots w_j) = p$ .

Preuve. Soient  $r_n = k_n$

$$r_{n-1} = k_n k_{n-1}$$

$$\vdots$$

$$r_0 = k_n k_{n-1} \dots k_0$$

Nous montrons, par récurrence descendante sur  $p$  :  $(*) \forall p \in \{0, \dots, n$

$\forall w \in X^*$  tel que  $r(w) = p$  et  $|w| \geq r_p$ ,  $w$  possède un facteur

$w_1 \dots w_{k_p}$  comme dans l'énoncé.





- Si  $r(w) = n$  et  $|w| \geq r_n = k_n$ ,  $w$  a un facteur  $x_1 \dots x_{k_n}$ ,  $x_i \in X$ . Mais alors  $\forall i \leq j$
- $$n \geq r(x_i \dots x_j) \geq r(w) = n \Rightarrow r(x_i \dots x_j) = n$$
- Soit  $0 \leq p < n$  et supposons que  $(*)$  soit vrai pour tous les  $p' > p$ . Soit  $w$  un mot tel que  $r(w) = p$  et  $|w| \geq r_p = k_p r_{p+1}$ ; alors  $w$  possède en facteur un mot  $w_1 w_2 \dots w_{k_p}$  tel que  $\forall i$ ,  $|w_i| = r_{p+1}$ . Si pour un  $i$ ,  $r(w_i) = p' \geq p+1$ , comme  $|w_i| = r_{p+1} \geq r_{p'}$ , on conclut par récurrence. Sinon,  $\forall i$ ,  $r(w_i) \leq p$ .

Mais alors  $\forall i \leq j$

$$p = r(w) \leq r(w_i \dots w_j) \leq r(w_i) \leq p, \text{ donc } r(w_i \dots w_j) = p. \square$$

Preuve du théorème 1. (i) Soit  $k_i = \binom{n}{i} + 1$  et  $N(n) = k_0 k_1 \dots k_n$ . Soit  $\mu: X^* \rightarrow K^{n \times n}$  et  $r: X^* \rightarrow \{0, 1, \dots, n\}$  défini par  $r(w) = \text{rang}(\mu w)$ . Soit  $w$  un mot de longueur au moins  $N(n)$ . D'après le lemme 1, il existe  $p$  tel que  $w$  possède en facteur un mot de la forme  $w_1 w_2 \dots w_{k_p}$  avec  $\forall i \leq j$ ,  $w_i \neq 1$  et  $r(w_i \dots w_j) = p$ .

(ii) Si  $p = 0$ ,  $r(w_1) = 0$  et  $\mu w_1 = 0$  est pseudo-régulière. Si  $p = n$ ,  $r(w_1) = n$  et  $\mu w_1$  est inversible, donc pseudo-régulière. Nous pouvons donc supposer

$$0 < p < n$$

(iii) Si  $E$  est un sous-espace de  $V = K^n$ , nous lui associons un élément  $\bar{E}$  de l'algèbre extérieure  $\wedge V$  de  $V$ , de la manière suivante : nous choisissons une base  $(v_1, \dots, v_k)$  de  $E$  et posons

$$\bar{E} = v_1 \wedge v_2 \dots \wedge v_k$$

( $\bar{E}$  ne dépend de cette base que par multiplication par un scalaire non nul).

On a  $\bar{E} \in \wedge^{\dim(E)} V$ .

Si  $E$  et  $F$  sont deux sous-espaces, on a

$$\bar{E} \wedge \bar{F} = 0 \iff E \cap F \neq 0$$

(voir Bourbaki, 1962, chap. 3, § 7, n° 3, prop. 5).

$$\begin{aligned} \text{(iv) Posons} \quad E_i &= \text{Im}(\mu w_i) \\ F_i &= \text{Ker}(\mu w_i) \end{aligned}$$

Nous avons  $\forall j, i \leq j \leq k_p - 1, r(w_j w_{j+1}) = r(w_j)$ ,

$$\text{donc } E_j \cap F_{j+1} = 0, \quad \text{donc } \bar{E}_j \wedge \bar{F}_{j+1} \neq 0$$

De plus,  $\forall i, j, 1 \leq i \leq j \leq k_p, r(w_i \dots w_j) = r(w_i) = r(w_j)$

$$\text{donc } \text{Im}(\mu w_i \dots w_j) = \text{Im}(\mu w_j) = E_j \quad \text{et} \quad \text{Ker}(\mu w_i \dots w_j) = F_i.$$

Supposons que pour tout  $i, j, 1 \leq i \leq j \leq k_p, \mu w_i \dots w_j$  ne soit pas pseudo-régulière. Alors  $\text{Im}(w_i \dots w_j) \cap \text{Ker}(w_i \dots w_j) \neq 0$  (prop. 1)

$$\text{donc } \bar{E}_j \wedge \bar{F}_i = 0, \quad \text{pour } i \leq j. \quad \text{Mais pour tout } j, \bar{F}_j \in \wedge^{n-p} V,$$

dont la dimension est  $\binom{n}{n-p} = \binom{n}{p} = k_p - 1$ . Il existe donc  $j$  tel que

$\bar{F}_{j+1}$  soit combinaison linéaire des  $\bar{F}_i, i \leq j$  :

$$\bar{F}_{j+1} = \sum_{i \leq j} \alpha_i \bar{F}_i \quad (\alpha_i \in K)$$

$$\text{Mais alors } \bar{E}_j \wedge \bar{F}_{j+1} = \sum_{i \leq j} \alpha_i \bar{E}_j \wedge \bar{F}_i = 0$$

ce qui est contradictoire.  $\square$

Nous sommes maintenant en mesure de démontrer le théorème d'itération qui est :

le résultat principal de ce paragraphe. Auparavant, nous avons besoin de quelques définitions :

soit  $w$  un mot de longueur  $k$  :  $w = x_1 \dots x_k$

( $x_i \in X$ ). Un ensemble de  $p$  positions marquées dans  $w$  est un sous-ensemble

$E$  de cardinalité  $p$  de  $\{1, \dots, n\}$  ; si  $w = aub$ , on dit que  $u$

contient  $q$  positions marquées si  $u = x_1 \dots x_j$  et  $E \cap \{i, i+1,$

$\dots, j\}$  est de cardinalité  $q$ .

Théorème 2. Soit  $X$  un alphabet et  $S \in K \langle\langle X \rangle\rangle$  une série reconnaissable. Il existe  $N$  tel que pour tout mot  $w \in \text{supp}(S)$  ayant au moins  $N+2$  positions marquées,  $w$  s'écrit  $aub$  où  $a$  (resp.  $b$ ) contient au moins une position marquée,  $u$  contient au moins une et au plus  $N$  positions marquées et où  $\text{supp}(S) \cap a u^* b$  est infini.

Preuve. Soit  $(\lambda, \mu, \gamma)$  une représentation linéaire de dimension  $n$  de la série  $S$ . Soit  $N = N(n)$  la constante du théorème 1' :  $w$  a une factorisation  $au_1 \dots u_N b$  où chaque  $u_i$  contient exactement une position marquée et où  $a$  (resp.  $b$ ) en contient au moins une. D'après le th. 3', il existe  $i \leq j$  tels que la matrice  $\mu u_i \dots u_j$  soit pseudo-régulière. On conclut alors en utilisant le lemme 1 du § 1, comme pour la preuve du th. 1, § 1.  $\square$

Remarque 2. Ce théorème admet comme conséquence le théorème 1 du § 1, comme on s'en convainc aisément.

Application. Considérons le langage (imaginé par Luc Boasson) suivant, sur l'alphabet  $\{x, y\}$ .

$$L = \{ yx^{i_1} yx^{i_2} \dots yx^{i_k} \mid k \geq 1 \text{ et } \forall j, 1 \leq j \leq k, i_j \geq j \}$$

Nous allons montrer que  $L$  n'est pas support d'une série rationnelle, et ce, en utilisant le théorème 2. Par ailleurs, nous verrons qu'on ne peut, pour arriver à cette conclusion, utiliser le th. 1 du § 1.

Si  $w = aub \in L$  et  $|u| \geq 2$ ,  $u$  contient au moins une occurrence de  $x$  donc  $u = u_1 x u_2$  et  $au_1 x^* u_2 b \subset L$ . Donc  $au_1 x^* u_2 b \cap L$  est infini et l'on ne peut utiliser le th. 1 du § 1 pour montrer que  $L$  n'est pas support d'une série rationnelle.

- Soit  $N \geq 1$  et  $w = yxyx^2 \dots yx^{N+2}$  où les  $N+2$  occurrences de  $y$  sont marquées. Si  $w = aub$  où  $u$  contient au moins un  $y$ , il n'est pas difficile de voir que pour  $n$  assez grand  $au^n b \notin L$ . Par suite,

$au^*b \cap L$  est fini, donc d'après le théorème 2,  $L$  n'est pas support d'une série rationnelle.

### 3. APPLICATIONS.

Nous étudions dans ce paragraphe les deux problèmes suivants :

- (i) Est-ce que l'image d'une série rationnelle par un morphisme de monoïdes libres est encore une série rationnelle ?
- (ii) Est-ce que l'image du support d'une série rationnelle par un tel morphisme est encore le support d'une série rationnelle ?

La première question n'a de sens que si l'image est définie. C'est le cas lorsque le morphisme est propre (i.e. l'image de toute lettre est un mot non vide) et dans ce cas, il est bien connu que la réponse est positive (voir par exemple Eilenberg 1974, prop. 4.8, chap. VII). Nous donnons ici une réponse positive dans le cas des morphismes quelconques, pourvu que l'image soit bien définie et que le demi anneau des coefficients est contenu dans un corps commutatif.

Quant à la deuxième question, on sait que la réponse est positive lorsque le demi anneau des coefficients est un sous-corps de  $\mathbb{R}$  (voir Salomaa et Soittola 1977, th. 2.4, chap. III). Nous étendons ce résultat au cas des sous demi-anneaux de  $\mathbb{R}$ .

Soit  $\varphi : X^* \rightarrow Y^*$  un morphisme de monoïdes libres et  $S \in K\langle\langle X \rangle\rangle$ . Rappelons que la famille de séries de  $K\langle\langle Y \rangle\rangle$

$$((S, w) \quad \varphi(w)) \quad w \in X^*$$

est dite *localement finie* si pour tout mot  $v \in Y^*$ , il n'y a qu'un nombre fini de mots  $w \in X^*$  tels que  $(S, w) \neq 0$  et  $\varphi(w) = v$ . Dans ce cas on définit la série image de  $S$  par  $\varphi$  par la formule

$$(\varphi(S), v) = \sum_{\varphi(w)=v} (S, w)$$

Théorème 1. On suppose que  $K$  est sous-*semi*-anneau d'un corps commutatif. Soit  $\varphi : X^* \rightarrow Y^*$  un morphisme de monoïdes libres et  $S \in K \langle\langle X \rangle\rangle$  une série rationnelle telle que la famille  $((S, w) \varphi(w))_{w \in X^*}$  soit localement finie. Alors  $\varphi(S)$  est une série rationnelle.

Preuve. (i)  $\varphi$  peut s'écrire comme produit d'un morphisme injectif suivi d'une projection. Par exemple, soit  $Z = X \cup Y$  (avec  $X \cap Y = \emptyset$ )

et

$$\psi : X^* \rightarrow Z^*$$

$$\pi : Z^* \rightarrow Y^*$$

définis par  $\psi(x) = x$  et  $\pi(y) = y$  pour  $x \in X$ ,  $\pi(y) = y$  si  $y \in Y$ . Alors  $\psi$  est injectif,  $\pi$  est une projection et  $\varphi = \pi \circ \psi$ . Comme  $\psi$  est injectif, la famille  $((S, w) \psi(w))_{w \in X^*}$  est localement finie et sa somme  $T = \psi(S)$  est une série rationnelle (voir Eilenberg, 1974, prop. 4.8, chap. VII). Par ailleurs, la famille  $((T, v) \pi(v))_{v \in Z^*}$  est localement finie, puisque  $\psi$  est injectif, et sa somme  $\pi(T)$  n'est autre que  $\varphi(S)$ . On est donc ramené à démontrer le théorème dans le cas où  $\varphi$  est une projection : il existe  $X' \subset X$  tel que  $X \setminus X' \subset Y$  et  $\forall x \in X'$ ,  $\varphi(x) = 1$  et  $\forall x \in X \setminus X'$ ,  $\varphi(x) = x$ .

(ii) Soit  $N$  la constante du théorème 1 du § 1. Alors  $\text{supp}(S) \subset X^* \setminus X'^N X^*$

En effet, supposons le contraire : il existe  $a, u, b \in X^*$  tels que  $u \in X'^N$  et  $aub \in \text{supp}(S)$ . D'après le théorème 1 du § 1,  $u$  se factorise en  $u_1 u_2 u_3$  tel que  $au_1 u_2^* u_3 b \cap \text{supp}(S)$  est infini. Mais on a  $\varphi(au_1 u_2^* u_3 b) = \varphi(ab)$  et il existerait une infinité de mots  $w$  tels que  $\varphi(w) = \varphi(ab)$  et  $(S, w) \neq 0$ .

(iii) On a donc, en particulier,

$$\text{supp}(S) \subset \bigcup_{\substack{|u| < N \\ u \in X'^N}} u (X \setminus X') X^*$$

et cette réunion est disjointe. Donc  $S = \sum S_u$  avec  $S_u = S \odot \underline{u(X \setminus X') X^*}$

$= u [(u^{-1}S) \odot (X \setminus X') X^*]$  où  $u^{-1}S$  est défini comme d'habitude par  
 $(u^{-1}S, w) = (S, uw)$ . Soit  $T_u = (u^{-1}S) \odot (X \setminus X') X^*$ , alors  $S = \sum_u T_u$   
 et  $\varphi(S) = \sum \varphi(T_u)$  puisque  $\varphi(u) = 1$  et que les séries  $\varphi(T_u)$   
 sont définies. Il suffit donc de montrer que  $\varphi(T_u)$  est rationnelle.

(iv) On a  $\text{supp}(T_u) \subset (X \setminus X') X^* \setminus X^* X'^N X^*$

Soit  $\alpha : (X \setminus X')^* \rightarrow K \langle X \rangle$

$$y \mapsto y \left( \sum_{\substack{u \in X'^* \\ |u| < N}} u \right)$$

Nous définissons comme d'habitude la série  $\alpha^{-1}(T_u) = T_u \circ \alpha : K \langle\langle X \setminus X' \rangle\rangle$   
 $\subset K \langle\langle Y \rangle\rangle$  par  $(\alpha^{-1}(T_u), v) = (T_u, \alpha(v))$  où  $T_u$  est considéré comme  
 forme linéaire sur  $K \langle X \rangle$ . Alors la série  $\alpha^{-1}(T_u)$  est rationnelle, puisque  
 si  $(\lambda, \mu, \gamma)$  est une représentation linéaire de  $T_u$ ,  $(\lambda, \alpha \circ \mu, \gamma)$   
 est une représentation linéaire de  $\alpha^{-1}(T_u)$ .

Par ailleurs, si  $v = y_1 \dots y_n$ , on a

$$\begin{aligned} (\varphi(T_u), v) &= \sum_{\varphi(w) = v} (T_u, w) \\ &= \sum_{\substack{u_1, \dots, u_n \in X'^* \\ |u_i| < N}} (T_u, y_1 u_1 y_2 \dots y_n u_n) \\ &= (T_u, \alpha(v)) = (\alpha^{-1}(T_u), v) \end{aligned}$$

Par suite  $\varphi(T_u) = \alpha^{-1}(T_u)$  est rationnelle.  $\square$

Théorème 2. On suppose que  $K$  est un sous-demi anneau de  $\mathbb{R}$ . Alors l'image  
 par tout morphisme de monoïdes libres de tout langage qui est support d'une  
 série  $K$ -rationnelle est encore le support d'une série  $K$ -rationnelle.

Corollaire. ( $K$  sous-demi anneau de  $\mathbb{R}$ ). La famille des langages qui sont  
 support de série  $K$ -rationnelle est un cône rationnel fermé pour les opérations  
 rationnelles.

Preuve. Que la famille considérée soit fermée pour les opérations rationnelles résulte de constructions déjà utilisées par Schützenberger (1961). De même, elle est fermée par intersection avec un langage rationnel et par morphisme inverse : les constructions sont immédiates. Elle est, de plus, fermée par morphisme direct (théorème 2), donc par toute transduction rationnelle.  $\square$

Preuve du théorème 2. Comme tout morphisme est produit d'un morphisme injectif et d'une projection, et que le cas d'un morphisme injectif est évident, nous sommes ramenés au cas d'une projection ; nous pouvons même supposer que la projection n'efface qu'une seule lettre. Soit donc  $Y$  un alphabet,  $X = Y \cup x$ , où  $x \notin Y$ ,  $\varphi : X^* \rightarrow Y^*$  la projection :  $\varphi|_Y = \text{id}$ ,  $\varphi(x) = 1$ . Soit  $L$  un langage qui est support d'une série  $K$ -rationnelle. Comme le carré d'Hadamard d'une série rationnelle est une série rationnelle, on peut supposer que  $L = \text{supp}(S)$  où  $S$  est une série  $K$ -rationnelle à coefficients non négatifs. Soit  $(\lambda, \mu, \gamma)$  une représentation linéaire de  $S$  de dimension  $n$  et  $A$  le langage

$$A = X^* \setminus X^* x^n X^*$$

Alors pour tout  $w \in \text{supp}(S)$ , il existe  $w' \in \text{supp}(S) \cap A$  tel que  $\varphi(w') = \varphi(w)$ . En effet, si  $w = ax^n b \in \text{supp}(S)$ , par le théorème de Hamilton-Cayley,  $(S, w)$  est combinaison linéaire des  $(S, ax^i b)$ ,  $i < n$ . Il existe donc  $i < n$  tel que  $ax^i b \in \text{supp}(S)$  ; de plus,  $\varphi(w) = \varphi(ax^i b)$ .

On a donc  $\varphi(L) = \varphi(A \cap L) = \varphi(\text{supp}(T))$

où  $T = S \otimes \underline{A}$  est  $K$ -rationnelle.

La famille  $((T, w) \varphi(w))_{w \in X^*}$  est clairement localement finie, puisque  $\text{supp}(T) \subset A$ . Par suite,  $\varphi(T)$  est une série  $K$ -rationnelle. Or,  $\varphi(\text{supp}(T)) = \text{supp}(\varphi(T))$  puisque les coefficients de  $T$  sont non négatifs.  $\square$

4. COMPLEMENTATION.

Le complémentaire du support d'une série rationnelle n'est en général pas support d'une série rationnelle : on peut, pour le voir, considérer la série  $\sum_w (|w|_x - |w|_y) w$  sur l'alphabet  $\{x, y\}$ ; le complémentaire de son support n'est pas support, d'après le théorème 1 du § 1. Cependant, l'on sait que le complémentaire d'un langage rationnel est un langage rationnel. Par ailleurs, le lecteur n'est certainement pas sans avoir remarqué l'analogie au moins formelle, entre supports de séries et complémentaires de variétés algébriques. De manière précise, soient  $P$  et  $Q$  deux polynômes en  $k$  variables commutatives à coefficients dans le corps commutatif  $K$ . Soient  $S$  et  $T$  les séries sur l'alphabet  $X = \{x_1, \dots, x_k\}$

$$S = \sum_{w \in X^*} P(|w|_{x_1}, \dots, |w|_{x_k}) w$$

$$T = \sum_{w \in X^*} Q(|w|_{x_1}, \dots, |w|_{x_k}) w$$

$S$  et  $T$  sont des séries rationnelles. Si  $\text{supp}(S) \cap \text{supp}(T) = \emptyset$ , on a pour tous entiers naturels  $a_1, \dots, a_k$  :  $(PQ)(a_1, \dots, a_k) = 0$ , donc  $PQ = 0$  et par suite, soit  $S = 0$ , soit  $T = 0$ .

La question que nous posons concerne les couples de langage qui sont à la fois disjoints et supports de séries rationnelles. Il n'est pas vrai, en général, qu'alors l'un des deux est vide, comme c'est le cas dans l'exemple ci-dessus. Mais nous proposons la conjecture suivante (les séries rationnelles considérées dans ce paragraphe le sont sur un corps commutatif).

Conjecture 1. Si  $L_1$  et  $L_2$  sont deux langages disjoints et supports de séries rationnelles, il existe un langage rationnel contenant  $L_1$  et ne contenant pas  $L_2$  (i.e.  $L_1$  et  $L_2$  sont rationnellement disjoints).

Remarque 1. Si  $L_1 = \text{supp}(S_1)$ ,  $L_2 = \text{supp}(S_2)$ ,  $L_1$  et  $L_2$  sont disjoints si et seulement si  $S_1 \odot S_2 = 0$ . La conjecture ci-dessus est donc liée au problème des diviseurs de zéro dans l'algèbre de Hadamard des séries rationnelles (voir § 3, chap. 6).

Une conjecture plus faible que la précédente est la suivante.

Conjecture 2. Si  $L_1$  et  $L_2$  sont deux langages complémentaires et tous deux supports de séries rationnelles, alors ils sont rationnels.

Nous allons démontrer ces conjectures dans des cas particuliers. Remarquons que si  $K$  est de caractéristique zéro et si  $L$  est un langage sur un alphabet à une seule lettre qui est support d'une série rationnelle,  $L$  est un langage rationnel (théorème de Skolem-Mahler-Lech, cf. Lech 1953). Dans ce cas, la conjecture est donc trivialement vérifiée (moyennant ce théorème..., qui ne s'étend pas à la caractéristique non nulle).

Théorème 1. Soient  $S, T \in K[[x]]$  rationnelles et telles que  $S \odot T = 0$ . Il existe deux séries rationnelles  $S' = \sum a_n x^n$  et  $T' = \sum b_n x^n$  telles que  $S - S'$  et  $T - T'$  soient des polynômes et un entier  $q \geq 1$  tel que pour tout  $i$ ,  $0 \leq i \leq q-1$ , on ait, ou bien  $a_{i+qn} = 0$  pour tout  $n$ , ou bien  $b_{i+qn} = 0$  pour tout  $n$  (ou les deux).

Corollaire. Si  $L_1, L_2$  sont deux langages disjoints contenus dans  $x^*$  et qui sont supports de séries rationnelles, alors il existe un langage rationnel contenant  $L_1$  et ne rencontrant pas  $L_2$ .

Preuve. Ceci vient du fait qu'une partie de  $x^*$  est rationnelle si et seulement si elle est égale, à un nombre fini d'éléments près, à une union finie de progressions arithmétiques.  $\square$

Preuve du théorème 1. (i) Il existe, d'après la proposition 4 du § 9, chap. I, des séries rationnelles régulières  $S'$  et  $T'$ , telles que  $S = S'$  et  $T = T'$  soient des polynômes. Alors  $S' \odot T'$  est une série rationnelle régulière et un polynôme, donc  $S' \odot T' = 0$  (prop. 5, § 9, chap. I).

(ii) D'après la proposition 3 du § 9, chap. I, il existe un entier  $N$  et des séries rationnelles  $S_0, \dots, S_{N-1}$ ,  $T_0, \dots, T_{N-1}$  telles que pour tout  $k$ , le couple  $(S_k, T_k)$  est normal et que  $S$  (resp.  $T$ ) est égale à l'emboîtement des séries  $S_0, \dots, S_{N-1}$  (resp.  $T_0, \dots, T_{N-1}$ ).

(iii) Pour conclure, il suffit de vérifier que si les couples de séries rationnelles  $(\bar{S}, \bar{T})$  est normal, alors  $\bar{S} \odot \bar{T} = 0$  implique  $\bar{S}$  ou  $\bar{T} = 0$ .

Rappelons que si  $G$  est un groupe abélien libre et  $A$  un anneau commutatif intègre, l'algèbre  $A[G]$  est sans diviseurs de 0, i.e.  $EF = 0$  implique  $E$  ou  $F = 0$ . Or, soient  $\lambda_1, \dots, \lambda_r$  (resp.  $\mu_1, \dots, \mu_s$ ) les racines de  $\bar{S}$  (resp.  $\bar{T}$ ). Le groupe  $G$  qu'elles engendrent est abélien libre. De plus, il existe, dans une extension  $L$  de  $K$ , des polynômes  $P_1(t), \dots, P_r(t)$  si la caractéristique de  $K$  est nulle (resp. des éléments  $P_1, \dots, P_r, Q_1, \dots, Q_s$  si la caractéristique de  $K$  est non nulle) tels que

$$\bar{S} = \sum_n (\lambda_1^n P_1(n) + \dots + \lambda_r^n P_r(n)) x^n, \quad \bar{T} = \sum_n (\mu_1^n Q_1(n) + \dots + \mu_s^n Q_s(n)) x^n$$

$$\text{(resp. } \bar{S} = \sum_n (\lambda_1^n P_1 + \dots + \lambda_r^n P_r) x^n, \quad \bar{T} = \sum_n (\mu_1^n Q_1 + \dots + \mu_s^n Q_s) x^n$$

Par suite, d'après la proposition 1 du § 9, chap. I (resp. la proposition 2 du § 9, chap. I) on a dans l'algèbre  $A[G]$ , où  $A = L[T]$  (resp.  $A =$  la relation

$$(\lambda_1 P_1(t) + \dots + \lambda_r P_r(t)) (\mu_1 Q_1(t) + \dots + \mu_s Q_s(t)) = 0$$

$$\text{resp. } (\lambda_1 P_1 + \dots + \lambda_r P_r) (\mu_1 Q_1 + \dots + \mu_s Q_s) = 0$$

D'après la remarque ci-dessus, il s'en suit que  $P_1 = \dots = P_r = 0$  ou  $Q_1 = \dots = Q_s = 0$ , donc  $\bar{S}$  ou  $\bar{T} = 0$ .  $\square$

Nous démontrons maintenant un résultat en rapport avec la conjecture 2, et obtenons comme corollaire une réponse positive à cette conjecture dans un cas particulier.

Théorème 2. Soient  $L_1$  et  $L_2$  deux langages complémentaires qui sont supports de séries rationnelles. Alors leur monoïde syntactique est un monoïde de torsion.

Remarque 2. Rappelons que deux langages complémentaires ont même monoïde syntactique.

Corollaire. Si  $L_1$  et  $L_2$  sont deux langages échangeables complémentaires et supports de séries rationnelles, ils sont rationnels.

Preuve. Le monoïde syntactique de  $L_1$  et  $L_2$  est commutatif ; par ailleurs, il est de torsion, donc il est fini et  $L_1$  et  $L_2$  sont rationnels.  $\square$

Lemme 1. Soient  $P, Q \in K[x]$ , non nuls, de degré majoré par  $m$ . Soient  $S = \sum a_n x^n$ ,  $T = \sum b_n x^n$  tels que  $P \circ S = 0$ ,  $Q \circ T = 0$  et que  $\forall n, a_n = 0 \Leftrightarrow b_n \neq 0$ . Soit  $L = \{n \mid a_n \neq 0\}$ . Il existe un entier  $N$  ne dépendant que de  $m$  et du corps engendré par les coefficients de  $P$  et  $Q$  tel que

$$\forall n \geq m, n \in L \Leftrightarrow n + N \in L.$$

Preuve. (i) D'après la proposition 4 du § 9, chap. I, il existe deux séries rationnelles régulières  $S'$  et  $T'$  telles que  $S - S'$  et  $T - T'$  soient des polynômes de degré  $\leq m - 1$ . En particulier,  $S'$  et  $S$  (resp.  $T'$  et  $T$ ) ont mêmes coefficients à partir du rang  $m$ . Comme les séries  $x^m \circ S' = x^m \circ S$

et  $x^m \circ T' = x^m \circ T$  sont régulières, on est ramené au cas où  $S$  et  $T$  sont régulières, pourvu qu'on montre

$$\forall n \geq 0, n \in L \Leftrightarrow n + N \in L.$$

(!!) Supposons donc  $S$  et  $T$  régulières. D'après la proposition 3 du § 9, chap. I il existe un entier  $N$ , ne dépendant que de  $m$  et du corps engendré par les coefficients de  $P$  et  $Q$ , et des séries rationnelles  $S_0, \dots, S_{N-1}$ ,  $T_0, \dots, T_{N-1}$  telles que, pour tout  $k$ , le couple  $(S_k, T_k)$  soit normal et que  $S$  (resp.  $T$ ) soit égale à l'emboîtement des séries  $S_0, \dots, S_{N-1}$  (resp.  $T_0, \dots, T_{N-1}$ ). On a alors, pour tout  $k$  :

$$\forall n, (S_k, x^n) = 0 \Leftrightarrow (T_k, x^n) \neq 0$$

Par suite,  $S_k \odot T_k = 0$ . On en déduit (cf. le point (iii) de la preuve du théorème 1)  $S_k = 0$  ou  $T_k = 0$  (ou exclusif). Donc  $L$  est réunion d'une classe modulo  $N$  et l'on peut conclure.  $\square$

Preuve du théorème 2. Soient  $S_1$  et  $S_2$  deux séries rationnelles telles  $L_1 = \text{supp}(S_1)$  et  $L_2 = \text{supp}(S_2)$ , et admettant respectivement les représentations linéaires  $(\lambda_1, \mu_1, \gamma_1)$  et  $(\lambda_2, \mu_2, \gamma_2)$  de dimension  $m$ . Soit  $w$  un mot et  $P$  (resp.  $Q$ ) le polynôme caractéristique de  $\mu_1 w$  (resp.  $\mu_2 w$ ). Soit  $N$  l'entier du lemme 1. Soient  $u, v$  des mots et

$$S' = \sum (S_1, uw^n v) x^n, \quad T' = \sum (S_2, uw^n v) x^n$$

On a  $P \circ S' = 0, \quad Q \circ T' = 0$  et

$$\forall n, (S_1, uw^n v) = 0 \Leftrightarrow (S_2, uw^n v) \neq 0$$

Par suite,

$$\forall n \geq m, uw^n v \in L_1 \Leftrightarrow uw^{n+N} v \in L_1$$

et ceci pour tous mots  $u, v$ . Ceci exprime que  $w^n$  et  $w^{n+N}$  sont dans la même classe de la congruence syntactique de  $L_1$ . Par suite, le monoïde syntactique de  $L_1$  est de torsion.  $\square$

5. EXTENSION

Soient  $L \supset K$  deux corps commutatifs. Si  $L$  est une extension algébrique de  $K$ , il n'est pas difficile de voir que tout langage qui est support d'une série  $L$ -rationnelle est aussi support d'une série  $K$ -rationnelle (on peut toujours supposer que  $[L : K] < \infty$ ; on étudie alors d'abord le cas des extensions galoisiennes, et le cas général se ramène à ce cas). Si  $L$  est une extension purement transcendante de  $K$ , un exemple de Lech (1953) montre qu'en caractéristique non nulle, il existe un langage qui est support de série  $L$ -rationnelle sans être celui d'une série  $K$ -rationnelle. Le cas de la caractéristique nulle est ouvert; le langage décrit dans la suite me semble être candidat à ne pas être support d'une série  $\mathbb{Q}$ -rationnelle, tout en étant support d'une série  $\mathbb{Q}(\alpha)$ -rationnelle, où  $\alpha$  est transcendant :

Soit  $S$  la série  $\mathbb{Q}(\alpha)$ -rationnelle sur l'alphabet  $X = \{x, y\}$

$$\begin{aligned} S &= (x^+ y^+)^* ((\alpha x)^+ y^+ - x^+ (\alpha y)^+) (x^+ y^+)^* \\ &= \sum_{k \geq 1} (\alpha^{i_1} + \dots + \alpha^{i_k} - \alpha^{j_1} - \dots - \alpha^{j_k}) x^{i_1} y^{j_1} \dots x^{i_k} y^{j_k} \\ &\quad i_1, j_1, \dots, i_k, j_k \geq 1 \end{aligned}$$

Soit  $A = \text{supp}(S)$

On a :

$$\begin{aligned} X^* \setminus A &= yX^* \cup X^*x \cup \{ x^{i_1} y^{j_1} \dots x^{i_k} y^{j_k} \mid \exists \sigma \in \mathfrak{S}_k \text{ tel que} \\ &\quad \forall h, 1 \leq h \leq k, \sigma(i_h) = j_h \} \end{aligned}$$

Question : Le langage  $A$  est-il support d'une série  $\mathbb{Q}$ -rationnelle ?

La proposition qui suit montre que, dans certains cas, des propriétés arithmétiques des coefficients d'une série rationnelle impliquent la rationalité du support.

Proposition 1. Soit  $S$  une série  $\mathbb{Z}$ -rationnelle possédant la propriété suivante : il existe un entier  $d \geq 1$  tel qu'aucun coefficient non nul de  $S$  ne soit divisible par  $d$ . Alors le support de  $S$  est un langage rationnel.

Preuve. On a en effet :

$$\forall w \in X^*, \quad (S, w) = 0 \iff (S, w) \equiv 0 \pmod{d}$$

Or, la série  $\bar{S}$  image de  $S$  par l'homomorphisme canonique  $\mathbb{Z} \rightarrow \mathbb{Z}/d\mathbb{Z}$  est  $(\mathbb{Z}/d\mathbb{Z})$ -rationnelle, donc son support est un langage rationnel puisque  $\mathbb{Z}/d\mathbb{Z}$  est fini. La relation ci-dessus exprime que  $\text{supp}(S) = \text{supp}(\bar{S})$ , donc  $\text{supp}(S)$  est rationnel.  $\square$

CHAPITRE VIII :     SUR LES SERIES ASSOCIEES A CERTAINS SYSTEMES DE  
LINDENMAYER.

Ce chapitre constitue un exemple d'application des séries rationnelles. Il concerne les DTOL-systemes, qui sont considérés ici comme des homomorphismes d'un monoïde libre  $Y^*$  dans le monoïde des endomorphismes d'un monoïde libre  $X^*$  ; lorsqu'on se donne en plus un mot privilégié de  $X^*$ , appelé l'axiome on obtient, par composition, une application de  $Y^*$  dans  $X^*$ . Si  $S$  est une série formelle  $S$  sur  $X$ , on obtient une série formelle  $T$  sur  $Y$ . Nous montrons que  $T$  est rationnelle dès que  $S$  est rationnelle à croissance polynômiale. Toute les constructions employées sont effectives, comme le lecteur peut s'en convaincre : ceci est illustré par un exemple au paragraphe 3.

Tous les alphabets considérés sont finis.

# 1. Séries $\mathbb{N}$ -rationnelles à croissance polynômiale.

Si  $S \in \mathbb{N} \langle\langle X \rangle\rangle$ , nous appelons *rang* de  $S$ , la dimension minimum d'une représentation linéaire de  $S$ . Par ailleurs, rappelons qu'une série  $T \in \mathbb{Z} \langle\langle X \rangle\rangle$  est dite à *croissance polynômiale* s'il existe des réels  $a, b \geq 1$  tels que

$$\forall w \in X^+, |(T, w)| \leq a |w|^b$$

Les séries  $\mathbb{Z}$ -rationnelles à croissance polynômiale ont été étudiées de manière très précise par Schützenberger (1962) qui a montré que les différents entiers traduisant la vitesse de croissance d'une telle série sont tous égaux. D'autres études sur ce sujet se trouvent dans Eilenberg (1974, ex. 1.2.3 du § 9, chap. VII), Ruohonen (1975 § 4), Salomaa et Soittola (1977 th. 9.9 et ex. 10.3 du chap. II) et Reutenauer (1977 chap. II et 1978).

Exemple 1 (i) La série

$$\sum_{w \in X^*} |w| w$$

est évidemment à croissance polynômiale.

(ii) Pour  $w, v \in X^*$ , soit  $\binom{w}{v}$  le *coefficient binomial* (voir par exemple Eilenberg 1974 chap. VII § 10) : il désigne le nombre de fois que  $v$  apparaît comme sous mot de  $w$

i.e.

$$\binom{w}{1} = 1 \text{ et si } v = x_1 x_2 \dots x_n \quad (x_i \in X)$$

$$\binom{w}{v} = \text{Card} \{ (u_0, \dots, u_n) \mid w = u_0 x_1 u_1 \dots x_n u_n, u_i \in X^* \}$$

On a  $\binom{w}{v} \leq \binom{|w|}{|v|}$  avec égalité si  $w$  et  $v$  sont puissance d'une même lettre. Par suite, la série

$$\sum_{w \in X^*} \binom{w}{v} w$$

est à croissance polynômiale.

Nous démontrons maintenant que le  $\mathbb{N}$ -module, (noté  $\mathcal{H}_n$ ) engendré par les séries  $\mathbb{N}$ -rationnelles à croissance polynômiale et de rang  $\leq n$  est de type fini. Ceci peut être rapproché du fait suivant :

le  $\mathbb{N}$ -module des polynômes à coefficients entiers et de degré  $\leq n$  est de type fini.

Définition 1 Une série  $S \in \mathbb{N}\langle\langle X \rangle\rangle$  est dite *élémentaire d'ordre  $\leq n$*  s'il existe un homomorphisme  $\mu : X^* \rightarrow \mathbb{N}^{n \times n}$  tel que  $\mu X^* \subset \{0, 1\}^{n \times n}$  et  $i, j$  tels que pour tout mot  $w$ ,  $(S, w) = (\mu w)_{i, j}$ .

Une série élémentaire est la série caractéristique d'un langage : elle est donc à croissance polynômiale. De plus, elle est  $\mathbb{N}$ -rationnelle, donc le langage est rationnel. De manière précise, on peut montrer qu'une série caractéristique d'un langage rationnel est élémentaire si et seulement si, soit le mot vide n'est pas dans le langage, soit le langage est un sous-monoïde libre (voir Eilenberg 1974 prop. 6.6 chap. VI et Perrin 1977 corollaire 4.3. chap. II).

Définition 2 Une *série binômiale généralisée d'ordre  $\leq n$*  est une série de la forme

$$S_1 x_1 S_2 \dots x_{p-1} S_p$$

où les  $x_i$  sont des lettres et les  $S_i$  des séries élémentaires d'ordre  $\leq n_i$  avec  $n_1 + n_2 + \dots + n_p \leq n$ .

Nous notons  $B_n$  l'ensemble des séries binômiales généralisées d'ordre  $\leq n$ .

Soit  $S$  la série caractéristique de  $X^*$ .  $S$  est élémentaire d'ordre 1.

Donc

$$T = S x_1 S \dots x_{p-1} S$$

est élémentaire d'ordre  $\leq p$ . Il n'est pas difficile de vérifier que

$$(T, w) = \binom{w}{x_1 \dots x_{p-1}}$$

est le coefficient binomial. La terminologie employée est ainsi justifiée.

Lemme 1 Toute série binomiale généralisée d'ordre  $\leq n$  est une série  $\mathbb{N}$ -rationnelle à croissance polynômiale de rang  $\leq n$ .

Démonstration. Soit  $T = S_1 x_1 S_2 \dots x_{p-1} S_p$  comme dans la définition 2.

Alors

$$(S_1 x_1 S_2 \dots x_{p-1} S_p, w) \leq (S x_1 S \dots x_{p-1} S, w) = \binom{w}{x_1 \dots x_{p-1}} \leq |w|^{p-1}$$

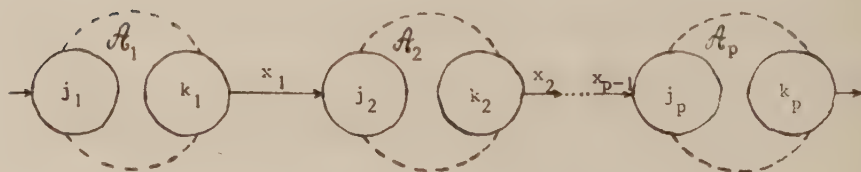
avec  $S = \underline{X}^*$ . Donc  $T$  est à croissance polynômiale. Il est de plus clair que  $T$  est  $\mathbb{N}$ -rationnelle. La série  $S_i$  est élémentaire d'ordre  $\leq n_i$ , donc il existe un morphisme  $\mu_i : X^* \rightarrow \mathbb{N}^{n_i \times n_i}$  et  $j_i, k_i$  tels que

$$(S_i, w) = (\mu_i w)_{j_i, k_i}$$

Soit  $\mathcal{A}_i$  le  $\mathbb{N}$ -automate associé à la représentation linéaire  $(\lambda_i, \mu_i, \gamma_i)$  ; pour des précisions à ce sujet on pourra consulter Eilenberg 1974 chap.

VI § 6. L'état initial de  $\mathcal{A}_i$  est  $j_i$  et son état final  $k_i$ .

Alors  $T$  est reconnue par l'automate  $\mathcal{A}$  suivant



L'automate  $\mathcal{A}$  a  $n_1 + \dots + n_p \leq n$  états donc  $T$  est de rang  $\leq n$ .  $\spadesuit$

Lemme 2  $B_n$  est fini.

Démonstration. Comme  $X$  est fini, il n'y a qu'un nombre fini d'homomorphismes  $\mu : X^* \rightarrow \mathbb{N}^{m \times m}$  tels que  $m \leq n$  et  $\mu X^* \subset \{0, 1\}^{m \times m}$ . Il n'y a donc qu'un nombre fini de séries élémentaires d'ordre  $\leq n$ . Ceci, joint à la finitude de  $X$ , implique qu'il n'y a qu'un nombre fini de séries binômiales généralisées d'ordre  $\leq n$ , i.e.  $B_n$  est fini.  $\spadesuit$

Lemme 3 Soit  $S$  une série  $\mathbb{N}$ -rationnelle à croissance polynômiale de rang  $\leq n$ . Alors  $S$  admet une représentation linéaire  $(\lambda, \mu, \gamma)$  de dimension  $\leq n$  et où  $\mu$  est sous la forme triangulaire par blocs.

$$\mu = \begin{pmatrix} \mu_1 & x & \dots & x \\ 0 & \mu_2 & & \vdots \\ & & \ddots & x \\ 0 & \dots & 0 & \mu_p \end{pmatrix}$$

avec, pour tout  $i$ ,  $\mu_i X^* \subset \{0, 1\}^{n_i \times n_i}$ .

Une démonstration de ce lemme peut être trouvée dans Reutenauer (1977 chap. II § 1)  $\spadesuit$

Lemme 4 Soit  $A$  un demi-anneau commutatif et  $\mu : X^* \rightarrow A^{n_1 \times n_1}$  un homomorphisme sous la forme

$$\mu = \begin{pmatrix} \mu' & \nu \\ 0 & \mu'' \end{pmatrix}$$

Alors toute série reconnue par  $\mu$  est une combinaison linéaire de séries reconnues par  $\mu'$ , par  $\mu''$  et de séries de la forme  $S' \times S''$  où  $S'$  est reconnue par  $\mu'$ ,  $S''$  par  $\mu''$  et où  $\times$  est une lettre.

Démonstration. Posons  $\bar{\mu} = \begin{pmatrix} \mu' & 0 \\ 0 & \mu'' \end{pmatrix}$  et  $\bar{v} = \begin{pmatrix} 0 & v \\ 0 & 0 \end{pmatrix}$

Alors, pour tous mots  $u, v, w$  on a :  $\bar{v} u \bar{\mu} v \bar{v} w = 0$ .

Par suite, si  $w = x_1 \dots x_n \in X^*$ , on a  $\mu w = \mu x_1 \dots \mu x_n = (\bar{\mu} x_1 + \bar{v} x_1) \dots$   
 $(\bar{\mu} x_n + \bar{v} x_n)$

$$= \bar{\mu} w + \sum_{\substack{w = uxv \\ u, v \in X^*, x \in X}} \bar{\mu} u \bar{v} x \bar{\mu} v$$

et le lemme en découle. 

Lemme 5 Toute série  $N$ -rationnelle à croissance polynômiale de rang  $\leq n$  est égale à une combinaison  $N$ -linéaire de séries binômiales généralisées d'ordre  $\leq n$ .

Démonstration. Soit  $S$  une telle série.  $S$  admet une représentation linéaire  $(\lambda, \mu, \gamma)$  de dimension  $m \leq n$  et qui vérifie les conclusions du lemme 3. Mais alors, il suffit d'appliquer itérativement le lemme 4 et l'on en déduit le lemme. 

Théorème 1 Le sous  $N$ -module  $\mathcal{M}_n$  de  $N\langle X \rangle$  engendré par les séries  $N$ -rationnelles à croissance polynômiale et de rang  $\leq n$  est de type fini : il est engendré par les séries binômiales généralisées d'ordre  $\leq n$ . De plus si  $S$  est dans  $\mathcal{M}_n$  et  $f : X^* \rightarrow X^*$  est un homomorphisme,  $S \circ f$  est encore dans  $\mathcal{M}_n$ .

Preuve D'après le lemme 1, toute série binômiale généralisée d'ordre  $\leq n$  est dans  $\mathcal{M}_n$  et d'après le lemme 5,  $\mathcal{M}_n$  est engendré par l'ensemble de ces séries, i.e.  $B_n$ ; comme  $B_n$  est fini (lemme 2)  $\mathcal{M}_n$  est un  $N$ -module de type fini. Soient  $S$  une série  $N$ -rationnelle à croissance polynômiale et de rang  $\leq n$  et  $f: X^* \rightarrow X^*$  un homomorphisme. Soit  $(\lambda, \mu, \gamma)$  une représentation de dimension  $\leq n$  de  $S$ . Alors  $S \circ f$  admet la représentation  $(\lambda, \mu \circ f, \gamma)$ . De plus, si  $\forall w \in X^+, (S, w) \leq a|w|^b$  alors  $(S \circ f, w) = (S, f(w)) \leq a|f(w)|^b$

Soit  $c = \sup \{|f(x)|, x \in X\}$

Alors  $|f(w)| \leq c|w|$ , donc

$(S \circ f, w) \leq a c^b |w|^b$  et  $S \circ f$  est à croissance polynômiale. Soit maintenant  $S \in \mathcal{M}_n$ ,  $S = \sum S_i$  où les  $S_i$  sont des séries  $N$ -rationnelles à croissance polynômiale et de rang  $\leq n$ . Alors les  $S_i \circ f$  sont encore ainsi, d'après ce qui précède, et

$$S \circ f = \sum S_i \circ f_i \in \mathcal{M}_n. \quad \square$$

## 2. DTOL-séries.

Définition 1 Un DTOL-système est un triplet  $G = (X, \{f_1, \dots, f_q\}, a)$  où  $X$  est un alphabet fini, chaque  $f_i$  un homomorphisme  $X^* \rightarrow X^*$  et  $a$  un élément de  $X^*$  appelé l'axiome. Si  $q = 1$  c'est un DOL-système. Soit  $Y = \{y_1, \dots, y_q\}$  un alphabet à  $q$  éléments. L'application

$$y_i \mapsto f_i$$

se prolonge en un homomorphisme de monoïdes:  $Y^* \rightarrow \text{Hom}(X^*)$ ; nous notons  $f_w$  l'image de  $w \in Y^*$ . Si  $S$  est une série formelle sur  $X$ , nous appelons transformée de  $S$  par  $G$ , notée  $G(S)$ , la série sur  $Y$  définie par

$$(G(S), w) = (S, f_w(a))$$

Exemple 1 Si  $G = (X, f, a)$  est un DOL-système et  $S = \sum |w| w$ , la transformée de  $S$  par  $G$  est la série d'une variable  $\sum |f^n(a)| y^n$ , courante dans l'étude des DOL-systèmes. Si  $S = \sum \binom{w}{v} w$  (cf. exemple 1 (ii) du § 1) alors  $G(S) = \sum (f_v^n(a)) y^n$ , dont Johansen (1978) prouve la rationalité et Ochsen schläger (1977) la  $\mathbb{N}$ -rationalité.

Nous montrons que, plus généralement, la transformée d'une série par un DTOL-système est  $\mathbb{N}$ -rationnelle, pour une large classe de série englobant celles de l'exemple ci-dessus.

Théorème 1 Soit  $G$  un DTOL-système  $S$  une série  $\mathbb{N}$ -rationnelle à croissance polynômiale. Alors la transformée de  $S$  par  $G$  est  $\mathbb{N}$ -rationnelle.

Remarque 1. La restriction sur la croissance n'est pas inutile, comme le montre l'exemple suivant :  $q = 1$ ,  $X = \{x\}$ ,  $f(x) = x^2$ ,  $a = x$ ,  $S = \sum 2^n x^n$ . Alors

$$G(S) = \sum 2^{2^n} y^n$$

qui n'est pas rationnelle, parce qu'elle croît trop vite (cf. prop. 5 du § 3 chap. I).

Démonstration Soit  $n$  tel que  $S \in \mathcal{M}_n$ . Si  $w \in Y^*$ , l'application

$$\begin{aligned} \mathcal{M}_n &\rightarrow \mathcal{M}_n \\ T &\mapsto T \circ f_w \end{aligned}$$

est  $\mathbb{N}$ -linéaire. De plus  $f_{ww} = f_w \circ f_w$ , donc  $T \circ f_{ww} = (T \circ f_w) \circ f_w$ . De cette manière,  $\mathcal{M}_n$  devient un  $\mathbb{N}\langle Y \rangle$ -module à droite.

Soit  $\varphi : \mathcal{M}_n \rightarrow \mathbb{N}$  la forme linéaire qui à  $T$  associe  $(T, a)$ , où  $a$  est l'axiome de  $G$ . Alors, pour tout mot  $w \in Y^*$ ,

$$(G(S), w) = (S, f_w(a)) = (S \circ f_w, a) = \varphi(S \circ f_w) \text{ donc } G(S) \text{ est}$$

$\mathbb{N}$ -rationnelle (prop. 1 (iv) § 3 chap. I).  $\square$

Corollaire 1 (Johansen 1978, Ochsen-schläger 1977) Soit  $G = (X, f, a)$  un DOL-système et  $v \in X^*$ . Alors la série  $\sum (f_v^n(a)) y^n$  est  $N$ -rationnelle.

Démonstration La série  $S = \sum_{w \in X^*} \binom{w}{v} w$  est  $N$ -rationnelle à croissance polynômiale, car c'est une série binômiale généralisée (cf. la remarque après la définition 2 § 1). La transformée de  $S$  par  $G$  n'est autre que  $\sum (f_v^n(a)) y^n$  et il suffit d'utiliser le théorème.

Corollaire 2 Soit  $G$  un DTOL-système et  $S$  une série  $Z$ -rationnelle à croissance polynômiale. La transformée de  $S$  par  $G$  est  $Z$ -rationnelle.

Démonstration D'après Schützenberger (1962a)  $S$  s'écrit  $S_1 - S_2$  où  $S_1$  et  $S_2$  sont  $N$ -rationnelles à croissance polynômiale. Mais alors  $G(S) = G(S_1) - G(S_2)$  est  $Z$ -rationnelle.

Corollaire 3 Soit  $G$  un DTOL-système et  $L \subset X^*$  un langage rationnel. Alors le langage  $G(L) = \{ w \in Y^* \mid f_w(a) \in L \}$  est rationnel.

Preuve La série caractéristique  $S$  de  $L$  est  $N$ -rationnelle (prop. 4 § 3 chap. I) à croissance polynômiale. La série  $G(S)$  est donc  $N$ -rationnelle. Or

$w \in \text{supp}(G(S)) \Leftrightarrow (S, f_w(a)) \neq 0 \Leftrightarrow f_w(a) \in L$  donc  $G(L) = \text{supp}(G(S))$  est rationnel.

Corollaire 4 Soit  $(X, f, a)$  un DOL-système et  $L \subset X^*$  un langage rationnel. Il existe des entiers  $h$  et  $p$  tels que

$$\forall n \geq h, f^n(a) \in L \Leftrightarrow f^{n+p}(a) \in L$$

Preuve Le langage sur  $y$

$$\{ y^n \mid f^n(a) \in L \}$$

est rationnel (corollaire 3). Le résultat découle donc du fait qu'une partie de  $\mathbb{N}$  est rationnelle si et seulement si elle union d'un ensemble fini et d'un nombre fini de progressions arithmétiques.

En fait, ces deux derniers résultats sont encore vrais dans un cadre bien plus général. Nous appelons *substitution* une application :  $X^* \rightarrow 2^{X^*}$  telle que  $f(uv) = f(u) f(v)$  pour tous mots  $u$  et  $v$ . L'ensemble des substitutions est un monoïde que nous notons  $\text{Sub}(X^*)$ .

Théorème 2 Soient  $f_1, \dots, f_q$  des substitutions  $X^* \rightarrow 2^{X^*}$  et  $a$  un mot dans  $X^*$ .

L'application  $y_i \mapsto f_i$  s'étend en un homomorphisme de monoïdes  $Y^* = \{y_1, \dots, y_q\}^* \rightarrow \text{Sub}(X^*)$ ; l'image de  $w$  est notée  $f_w$ . Soit

$L \subset X$  un langage rationnel. Alors le langage

$$\{w \in Y^* \mid f_w(a) \cap L \neq \emptyset\}$$

est rationnel.

Démonstration. Les automates considérés dans cette preuve sont les automates

non déterministes au sens habituel (cf. Eilenberg 1974 chap. II). Soit  $\mathcal{A} = (Q, q_0, Q_f, \lambda)$  un automate sur  $X$  et  $f : X^* \rightarrow 2^{X^*}$  une substitution. Nous notons  $\mathcal{A} \circ f$  l'automate

$$\mathcal{A} \circ f = (Q, q_0, Q_f, \lambda')$$

où  $\lambda'$  est défini par :  $\forall q, p \in Q, \forall x \in X \quad \lambda'(q, x) = p$  s'il existe  $v \in f(x)$  tel que  $\lambda(q, v) = p$ . Alors  $\mathcal{A} \circ f$  reconnaît le langage

$$L(\mathcal{A}) \circ f = \{v \mid f(v) \cap L(\mathcal{A}) \neq \emptyset\}$$

comme on le vérifie aisément. De plus, si  $g$  est une autre substitution

$$(\mathcal{A} \circ f) \circ g = \mathcal{A} \circ (f \circ g)$$

Soit  $\mathcal{A}_0$  un automate reconnaissant  $L$ , à  $n$  états. Soit  $\mathcal{M}$  l'ensemble fini des automates ayant  $n$  états. Alors l'application

$$\mathcal{M} \times Y^* \rightarrow \mathcal{M}$$

$$(\mathcal{A}, w) \mapsto \mathcal{A} \circ f_w$$

fait de  $\mathcal{M}$  un  $Y^*$ -module à droite. Soit

$$\mathcal{C} = (\mathcal{M}, \mathcal{A}_0, \mathcal{M}_f, \mu)$$

où  $\mathcal{M}_f = \{\mathcal{A} \in \mathcal{M} \mid \mathcal{A} \in L(\mathcal{A})\}$  et où  $\mu$  est défini par la structure de  $Y^*$ -module de  $\mathcal{M}$ .  $\mathcal{C}$  est un automate fini (et même déterministe) donc le

langage  $L(\mathcal{C})$  reconnu par  $\mathcal{C}$  est rationnel. Or

$$\begin{aligned} L(\mathcal{C}) &= \{ w \in Y^* \mid \mathcal{R}_0 \circ f_w \in \mathcal{M}_f \} \\ &= \{ w \in Y^* \mid a \in L(\mathcal{R}_0 \circ f_w) \} \\ &= \{ w \in Y^* \mid f_w(a) \cap L(\mathcal{R}_0) \neq \emptyset \} \quad \star \end{aligned}$$

### 3. Exemple

Soit  $X = \{x, y\}$  et  $G = (X, \{f, g\}, x)$  le DTOL-système défini par

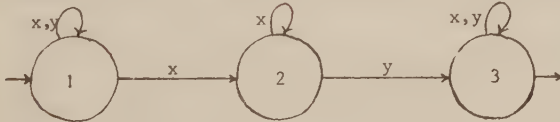
$$f(x) = xy, \quad f(y) = yx, \quad g(x) = yx, \quad g(y) = y.$$

Nous posons  $A = \{a, b\}$  et faisons correspondre  $f$  à  $a$  et  $g$  à  $b$ .

Soit  $S$  la série  $N$ -reconnaissable sur  $X$  définie par la représentation linéaire

$$\lambda = (1, 0, 0), \quad \mu x = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \mu y = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

A cette représentation linéaire est associé le  $N$ -automate.



qui met bien en évidence que

$$S = X^* x x^* y X^*$$

(cf. Eilenberg 1974 chap. VII § 6 et 7).

Autrement dit, pour tout mot  $w$ ,  $(S, w)$  est égal au nombre de factorisations

$$w = u x x^i y v$$

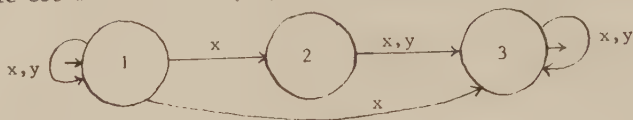
avec  $u, v \in X^*$ ,  $i \geq 0$ . On remarque aussi que  $S$  est une série binômiale généralisée.

Nous calculons  $S \circ f$  : cette série admet la représentation  $(\lambda, \mu', \gamma)$

avec

$$u'x = \mu \circ f(x) = \mu xy = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}, u'y = \mu yx = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

à laquelle est associé le N-automate



On a donc (ibid.)

$$S \circ f = X^* x X^* + X^* y^2 X^* + X^* y x X^*$$

De la même manière on démontre les formules

$$S \circ g = X^* x X^*$$

$$(X^* x X^*) \circ f = X^* x X^* + X^* y X^*$$

$$(X^* x X^*) \circ g = X^* x X^*$$

$$(X^* y X^*) \circ f = (X^* y X^*) \circ g = X^* x X^* + X^* y X^*$$

$$(X^* y x X^*) \circ f = X^* y X^* + X^* x^2 X^*$$

$$(X^* y x X^*) \circ g = X^* x^2 X^* + X^* y x X^*$$

$$(X^* x^2 X^*) \circ f = X^* y x X^*$$

$$(X^* x^2 X^*) \circ g = 0$$

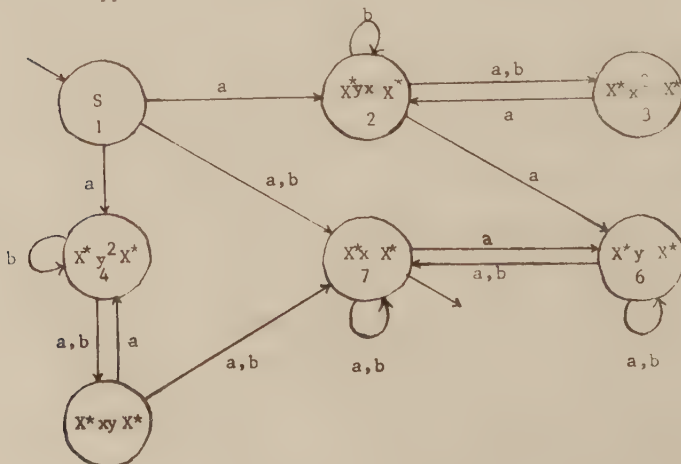
$$(X^* y^2 X^*) \circ f = X^* xy X^*$$

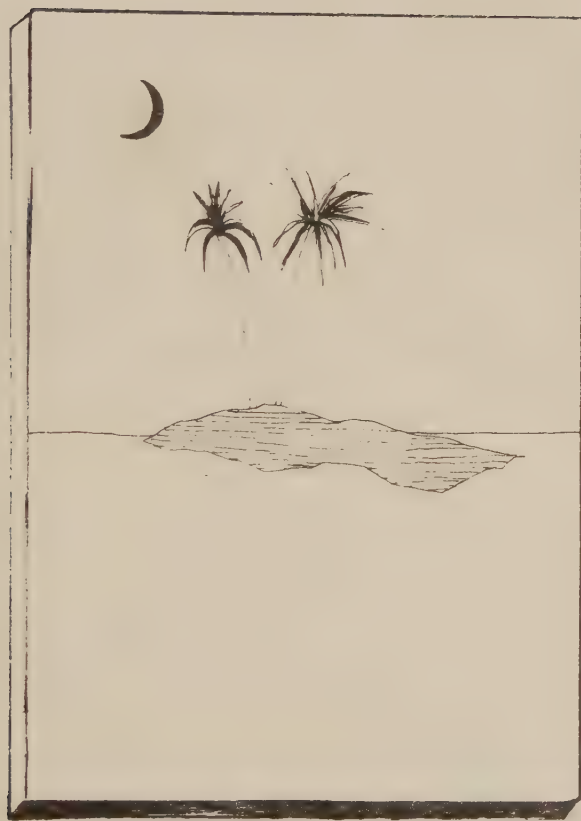
$$(X^* y^2 X^*) \circ g = X^* y^2 X^* + X^* xy X^*$$

$$(X^* xy X^*) \circ f = X^* y^2 X^* + X^* x X^*$$

$$(X^* xy X^*) \circ g = X^* x X^*$$

Par suite, la série  $G(S)$  est reconnue par le N-A-automate, dont les états sont les sept séries apparaissant dans les formules ci-dessus et dont l'état initial est  $S$  et l'état final  $X^* x X^*$ , car c'est la seule de ces séries dont le support contient l'axiome  $x$  (avec coefficient 1).







On a donc, pour  $G(S)$ , la représentation linéaire  $(\bar{\lambda}, \bar{\mu}, \bar{\gamma})$  avec

$$\bar{\lambda} = (1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0)$$

$$\bar{\mu}_a = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}, \bar{\mu}_b = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \bar{\gamma} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

On peut alors montrer (ibid.) que

$$G(S) = ((a(b+(a+b)a)^*) (a(a+b)^* + (a+b)) + 1) (a+b) ((1+a(a+b)^*) (a+b))^*$$



REFERENCES

- BENZAGHOU B. (1970) : Algèbres de Hadamard, Bull. Soc. math. France 98 209-252.
- BERSTEL J. (1970) : Séries formelles, manuscrit non publié.
- " (1971) : Sur les pôles et le quotient de Hadamard de séries N-rationnelles, C.R. Acad. Sci. Paris 272 1079-1081.
- " (1979) : Transductions and context-free languages, Teubner, Stuttgart.
- BOURBAKI N. (1961) : Algèbre commutative, Hermann, Paris.
- " (1962) : Algèbre, Hermann, Paris.
- CANTOR D.G. (1965) : On arithmetic properties of coefficients of rational functions, Pacific J. Math 15 55-58.
- CAHEN P.J. et J.L. CHABERT (1975) : Eléments quasi-entiers et extensions de Fatou, J. Algebra 36 185-192.
- CHABERT J.L. (1972) : Anneaux de Fatou, Enseignement Math. 18 (2) 141-144
- CHIRCHOV A.I. (1957) : On rings with identity relations, Mat. Sb. N.S. 43 (85) 277-283.
- CHOFFRUT C. (1978) : Thèse Doctorat d'Etat, Université Paris 7.
- " (1978a) : Sur les transductions reconnaissables, R.A.I.R.O. Informatique théorique 12 n° 3 203-212.
- COHN P.M. (1969) : Free associative algebras, Bull. London Math. Soc. 1 1-39.
- CORI R. et J. RICHARD (1972) : Enumération des graphes planaires à l'aide des séries formelles en variables non commutatives ; Discrete Math. 2 115-162.
- CURTIS C.W. et I. REINER (1962) : Representation theory of finite groups and associative algebras, Interscience Publishers, New York, London.
- EILENBERG S. (1974) : Automata, languages and machines, vol. A, Acad. Press, New York.

- EILENBERG S. (1976) : idem, vol. B.
- EILENBERG S. et M.B. SCHÜTZENBERGER (1969) : Rational sets in commutative monoids, J. Algebra 13 173-191.
- FATOU P. (1904) : Sur les séries entières à coefficients entiers, C.R. Acad. Sci. Paris Sér. A 138 342-344.
- FLIESS M. (1972) : Thèse de Doctorat d'Etat, Université Paris 7.
- " (1974) : Matrices de Hankel, J. Maths Pures Appl. 53 197-224.
- " (1974a) : Sur divers produits de séries formelles, Bull. Soc. math. Fr. 102 181-191.
- " (1974b) : Propriété booléenne des langages stochastiques, Maths. System Theory 7 353-359.
- " (1976) : Un outil algébrique : les séries formelles non commutatives, Lecture Notes Econom. Math. System 131 Springer Verlag, 122-148.
- GODEMENT R. (1966) : Cours d'algèbre, Hermann, Paris.
- HERSTEIN I.N. (1968) : Noncommutative rings, Carus Mathematical Monograph.
- HIGMAN G. (1952) : Ordering by divisibility in abstract algebras, Proc. London Math. Soc. 2 326-336.
- HOTZ G. (1976) : Der Satz von Chomsky-Schützenberger und die Schwerste Kontext-freie Sprache von S. Greibach, Asterisque, Soc. Math. France 38-39 105-115.
- JACOB G. (1975) : Sur un théorème de Shamir, Information and Control 27, 218-261.
- " (1975a) : Thèse Doctorat d'Etat, Université Paris 7.
- " (1978) : La finitude des représentations linéaires des semigroupes est décidable, J. Algebra 52 437-459.
- " (197X) : Un théorème de factorisation des produits d'endomorphisme, J. Algebra (à paraître).
- JOHANSEN P. (1979) : The generating function of the number of subpatterns of a DOL sequence, Théor. Comput. Sci. 8 (1) 57-68.
- KAPLANSKY I. (1969) : Fields and rings, Chicago lectures in Mathematics.
- KARHUMAKI J. (1977) : Remarks on commutative N-rational series, Theor. Comput. Sci. 5 211-217.

- LANECHE K. (1973) : Quelques propriétés des séries rationnelles en variables non commutatives, J. Combinatorial Theory (A) 14 128-135.
- LAMPERTI J. (1958) : On the coefficients of reciprocal power series, Amer. math. Monthly 68 90-94.
- LECH C. (1953) : A note on recurring series Arkiv Matematik 2 417-421.
- LEWIN J. (1969) : Free modules over free algebras and free group algebras : the Schreier technique, Trans. Amer. Math. Soc. 145, 455-465.
- LYNDON R.C. and P.E. SCHUPP : Combinatorial group theory, Springer-Verlag, Berlin, Heidelberg, New York.
- OCHSENSCHLÄGER P. (1977) : Verallgemeinerte Parikh-Abbildungen und DOL-systeme, Bericht AFS-33, Fachbereich Informatik, Technische Hochschule Darmstadt.
- PATHIAUX G. (1968) : Algèbre de Hadamard de fractions rationnelles, C.R. Acad. Sci. Paris Sér. A 267 977-980.
- PERRIN D. (1977) : Codes et combinatoires du monoïde libre, Cours de DEA Université Paris 7.
- PERROT J.-F. (1978) : Variétés de langages et opérations, Théor. Comput. Sci 7 197-210.
- PIN J.-E. (1980) : Variétés de langages et monoïdes des parties, Semigroup Forum (à paraître).
- PISOT C. (1959) : conférences données à l'Institut Fourier de Grenoble (miméogr.).
- PÓLYA G. (1921) : Arithmetische Eigenschaften der Reihenentwicklungen rationaler Funktionen, J. für reine und angewandte Math. 151 1-31.
- PÓLYA G. et G.SZEGO (1964) : Aufgaben und Lehrsätze aus der Analysis, Springer Verlag.
- PROCESI C. (1973) : Rings with polynomial identities, Dekker, New York.
- RANUM A. (1909) : The group membership of singular matrices, Amer. J. of Maths 31 18-41.
- REDEI L. (1965) : The theory of finitely generated commutative semigroups, Oxford, Edinburgh, New York.

REUTENAUER C. (1977) : Thèse 3ème cycle, Université Paris 6.

" (1978) : Une caractérisation des anneaux de Fatou faible,  
C.R. Acad. Sci. Paris Sér. A 287 295-296.

" (1978a) : Polynômes et séries formelles d'après Cohn, Bergman  
et Fliess, Actes du séminaire d'Informatique Théorique  
77-78, Université Paris 6.

" (1978b) : Sur les séries rationnelles en variables non commu-  
tatives, Lecture Notes in Comput. Sci. 62 372-381.

" (1979) : Sur les séries associées à certains systèmes de  
Lindenmayer, Theor. Comput. Sci. 9 363-375.

" (1979a) : Sur les séries de Pólya en variables non commutatives,  
Fundamental of computation theory 2 391-396, Akademie  
Verlag, Berlin.

" (1980) : An Ogden-like iteration lemma for rational power series,  
Acta Informatica (à paraître).

RUOHONEN K. (1975) : On the synthesis of DOL growth, Ann. Acad. Sci. Fenn.  
Ser. A I Math, 143-154.

SAKAROVITCH J. (1978) : Sur les monoïdes commutatifs, Séminaire d'Informati-  
que Théorique, Université Paris 6.

" (1979) : Monoïdes pointés, Semigroup Forum 18 235-264.

SALOMAA A. et M. SOITTOLA (1977) : Automata-theoretic aspects of formal  
power series, Springer Verlag, New York, Heidel-  
berg, Berlin.

SCHUTZENBERGER (1961) : On the definition of a family of automata, Informa-  
tion and Control 4 245-270.

" (1961a) : On a special class of recurrent events, Annals of  
Maths Statist, 32 1201-1213.

" (1962) : On a theorem of R. Jungen, Proc. Amer. Math. Soc.  
13 885-889.

" (1962a) : Finite counting automata, Information and Control  
5 91-107.

" (1965) : On finite monoïds having only trivial subgroups,  
Information and control 8 190-194.

- SHYR H.J. et G. THIERRIN (1974) : Hypercodes, Information and Control 24  
45-54.
- SONTAG E. (1975) : On some questions of rationality and decidability, J.  
Comput. System. Sci. 11 375-385.
- SONTAG E. et Y. ROUCHALEAU : Sur les anneaux de Fatou forts, C.R. Acad. Sci.  
Paris Sér. A 284 331-333.
- STEINBY M. : Syntactic algebras and varieties of subsets of algebras,  
Actes du colloque "Arbres en algèbre et en programmation",  
Lille (1979) 226-240.
- STRAUBING H. : Aperiodic homomorphisms and the concatenation product of  
recognizable sets, J. Pure Applied Alg. 15 319-327.













